

Año I nº I
2002
Distribución Gratuita
WINDOWS 2000
Active Directory el mayor cambio desde NT 4.0
certificaciones
Las 10 más buscadas
LINUX
¿Y para que necesito un Firewall
COR Technologies
NEX
PERIODICO DE NETWORKING
nº I
Adobe
Archivo Edición Imagen Capa Selección Filtro Vista Ventana Ayuda
Píxeles reales
Encajar en pantalla
Tamaño de impresión
tapa2.tif @ 33,3% (Capa 1,RGB)
INTRUSION DETECTION SYSTEMS
Que hacen y como trabajan
NEX CONNEXION

SUMARIO

editorial

Hoy NEX aparece por primera vez como un "Perisdico de Networking, Seguridad y Programacisn".
La pregunta es a quien esta dirigido y cual es el nivel de sus artículos.

El contenido de NEX apunta a aquellos con interés y que están activos en redes y programacisn. También será de mucha utilidad para estudiantes universitarios de las carreras de sistemas y/o buscando las certificaciones internacionales de CISCO, Microsoft (MCSE, MCSA, MCSD, MCDBA), Linu (LPI, Linu +) y otras.

Los artículos serán de un nievel intermedio y avanzado. En muchos habrá un recuadro con una introduccisn al tema. Los artículos que e cedan el espacio físico del perisdico podrán ser bajados íntegros desde nuestra pagina en Internet: www.ne web.com.ar

NEX trata de llenar un espacio NO cubierto por otras publicaciones del mercado y a su vez orientar en bibliografía, cursos y carrera a aquellos que se encuentren interesados en Information Technology (IT).

Muchas veces usaremos términos en ingles ya que creemos que toda persona con altas miras en esta actividad deberá de a poco lograr un dominio del idioma inglés. De este modo podrá por ejemplo aprovechar en su totalidad la vasta informacisn que aparece en Internet .

Buscaremos un balance entre los diferentes sistemas operativos que hoy rigen el mercado LINUX y Windows.

Seguridad en redes constituye hoy un tema de muchísima vigencia y haremos un especial énfasis en desarrollar temas de seguridad.

Temáticas relacionadas a web-design estaran tambien dentro de nuestro foco.

Esperamos contar con Uds para tener un feedback a nuestra oferta. No duden en contactarnos y aquellos que quieran recibir este perisdico pueden solicitarlo a través de nuestro web site.

Staff

Año 1 Nº 1 2002

Director
Dr. Carlos Osvaldo Rodríguez

Propietarioó
COR Technologies S.R.L.

Jefe de Redacción
Leonardo A. Costa

Relacioneó Públicaó
Cristina Rodríguez

Redactoreó
Carlos Osvaldo Rodríguez
Leonardo A. Costa
Marcelo Guazzardo

Colaboradoreó
Guillermo L. Mauro José Gatti
Oscar Raimundo

Dióeño Web SIte
Emanuel A. Rincsn

Dióeño Gráfico
Marcos Ferrer

Preimpreóión e Impreóión
Edigráfica s.a. Tel:4846236

Perisdico de Networking y Programacisn
Registro de la propiedad Intelectual en trámite
Direccisn: Csrdoba 657 12°
Capital Federal Tel:(011) 43127694
http: www.ne web.com.ar

El staff de Ne colabora ad-honorem, si querés escribir para nosotros enviar un e-mail a:
ne webs@yahoo.com.ar
Tirada de esta edicisn: 5000 ejem





Active Directory

Aparecido con la veróión 2000 de Windowó, Active Directory (AD) eó uno de loó mayoreó adelantoó de éóta veróión de Windowó con reópecto a óu anteceóor NT 4.0. AD eó una pieza clave dentro de la eótrategia de Microóoft para tranóformar a Windowó en un óiótema operativo empreóarial. Sin él muchaó de laó demáó parteó de eóa eótrategia no funcionarían. Laó group policieó (directivaó de grupo), laó jerarquíaó de loó dominioó, y la inótalación centralizada, no funcionarán haóta que el óiótema actúe como óervidor Active Directory.

AD es un servicio de Directorios de estructura jerárquica.

Es compatible con LDAP (Lightweight Directory Access Protocol - Protocolo Compacto de Acceso a Directorios). LDAP es un protocolo de acceso a listados de directorios. Es hermano de http y ftp, y el prefijo de sus URL es ldap://. También es compatible con NSPI (Name Service Provider Interface Interface de Proveedor de Servicios de Nombres), que es utilizado por los clientes de Microsoft E change 4.0 y 5. .

AD utiliza el sistema de resolucisn de nombres DNS (Domain Name Services - Servicios de Nombres de Dominios), el mismo que se utiliza en Internet. Esas características lo hacen muy adecuado para operar en ambientes de red heterogéneos incluyendo NDS (Novell Directory Services - Servicios de Directorios Novell) y NIS+ (Network Information Services - Servicios de Informacisn de Red - el servicio de nombres standard en sistemas Uni).

Active Directory admite el protocolo NSPI para proporcionar compatibilidad con el directorio de E change.

¿Que quiere decir todo esto?, Bueno, csmo DNS es un servicio de resolucisn de nombres, y AD lo usa, quiere decir que cada objeto que pertenezca al directorio va a poder ser ubicado por su nombre. Estos objetos pueden ser de muy diversas características. Se pueden publicar en el AD computadoras, usuarios, impresoras, servicios, shares (carpetas compartidas). De ésta forma cada objeto publicado en el AD, va a poder ser encontrado dentro de ese árbol sin importar donde se encuentre físicamente.

Con AD se acaba con las diferencias entre PDC (Primary Domain Controller - Controlador Primario del Dominio) y BDC (Backup Domain Controller - Controlador de Respaldo del Dominio), ya que lo que se tienen son DC (Domain Controllers - Controlador de Dominio) que almacenan sus datos en una base de datos compartida (el SYSVOL) que se encuentra replicada en todos los DC. Esta técnica provee tolerancia a fallos y velocidad de respuesta ya que la carga de trabajo se balancea automáticamente entre los DC.

El soporte de LDAP hace que clientes NO Microsoft, pero que también soporten LDAP (por ej.: Uni , Mac), podrán acceder a los objetos que se encuentren en el AD.

Active Directory
¿Qué eó un directorio?

En el conte to de las redes, un directorio (también llamado almacén de datos) es una estructura jerárquica que almacena informacisn de los *objetos* de la red. Los objetos pueden ser recursos compartidos como servidores, impresoras y carpetas compartidas; cuentas de usuarios y de computadoras; o también dominios, aplicaciones, servicios, políticas de seguridad y cualquier otra cosa que haya en la red. Un ejemplo típico de la informacisn que el directorio puede contener sobre un tipo particular de objeto son los datos de un usuario (nombre, direccisn, teléfono, e-mail). Siendo más mundanos, podemos decir que el término Directorio es utilizado con la acepcisn que se le da en el idioma inglés a la palabra directory, que se utiliza para nombrar la guía de teléfonos. Es decir un compendio organizado de entidades (usuarios) con sus datos asociados.

Un servicio de directorio no sslo almacena la informacisn, sino que también la hace disponible y utilizable para los usuarios, administradores, servicios de red y aplicaciones. Es decir que da estructura y soporte al funcionamiento de la red e interactúa con ella. En forma ideal un servicio de directorio hace transparente par el usuario la topología física y los protocolos de red, para que aquel puede acceder a los recursos sin necesidad de saber donde o csmo están físicamente conectados.

Algunos servicios de directorio están integrados a un sistema operativo mientras que otros están relacionados sslo con aplicaciones, por ejemplo los relacionados con clientes de e-mail. Los servicios de directorio de sistema operativo, como es Active Directory (AD), proveen administracisn de usuarios, computadoras y recursos compartidos. Los servicios de directorio que manejan e-mail (ej.: Microsoft E change) habilitan a los usuarios a buscar direcciones y enviar e-mails.

Active Directory, el nuevo servicio de directorio central de Windows 2000 Server, corre sslo sobre Domain Controllers (DC - Controladores de Dominio). Active Directory provee un lugar para almacenar datos y servicios que hacen disponibles esos datos, pero también brinda proteccisn contra accesos no autorizados a los datos y replica la informacisn de los objetos a otros DC a través de la red, así no hay pérdida de datos si un DC falla.

Ventajas de Active Directory

Seguridad de la información

El control de acceso (a través de las Access Control Lists - ACL) se puede definir para cada objeto del directorio y para cada una de sus propiedades. Active Directory proporciona el almacenamiento y el ámbito de aplicacisn para las directivas de seguridad. Las directivas de seguridad se aplican mediante la configuracisn de la Directiva de grupo.

Administración baóada en directivaó

El servicio de directorio de AD incluye un almacén de datos y una estructura jerárquica. Esto permite definir los conte tos en los que se aplican las directivas. Como directorio, almacena las directivas (denominadas objetos de Directiva de grupo) que se asignan a un conte to determinado. Un objeto de Directiva de grupo establece un conjunto de normas de empresa que incluyen opciones de configuracisn que pueden, en el conte to en que se aplican, determinar lo siguiente:

-El acceso a objetos de directorio y recursos del dominio

-Qué recursos del dominio, están disponibles para los usuarios

-Csmo se configuran esos recursos para su utilizacisn.

Capacidad de ampliación

El administrador de un AD tiene la posibilidad de agregar nuevas clases de objetos al schema (esquema) y nuevos atributos a las object classes (clases de objetos) ya e istentes.

Eócalabilidad

Un AD puede incluir uno o varios dominios, cada uno con uno o varios controladores de dominio, lo que permite escalar el directorio para satisfacer cualquier requisito de la red. En un árbol de dominios se pueden combinar múltiples dominios y múltiples árboles de dominios se pueden combinar en un bosque.

Replicación de la información

La replicacisn proporciona disponibilidad de la informacisn, tolerancia a errores, equilibrio de carga y mejoras en el rendimiento para el directorio. AD utiliza el sistema de replicacisn Multimaster, que permite actualizar el directorio en cualquier controlador de dominio, en lugar de en un solo controlador principal de dominio. La principal ventaja del modelo Multimaster es su mayor tolerancia a errores, ya que, con varios controladores de dominio, continúa la replicacisn aunque deje de funcionar uno de ellos.

Los DCs necesitan la informacisn más reciente del directorio, pero el intercambio indiscriminado de informacisn entre DCs puede sobrecargar la red. Por eso AD fue diseñado para replicar únicamente la informacisn de directorio que ha cambiado.



Integración con DNS

AD está integrado con DNS de las siguientes formas:

-Active Directory y DNS tienen la misma estructura jerárquica. Aunque son independientes y se implementan de forma distinta para propssitos diferentes, el namespace (espacio de nombres) de una organizacisn para DNS y Active Directory tienen una estructura idéntica.

-Las zonas DNS se pueden almacenar en AD. Si se utiliza el servicio DNS de Windows 2000, los archivos de zona primaria se pueden almacenar en Active Directory para su replicacisn en otros DC

-Los clientes de Active Directory utilizan DNS para encontrar a los DC. Para localizar un controlador de dominio determinado, los clientes de AD envían una consulta al servidor DNS.

Interoperabilidad con otroó óervicioó de directorio

Debido al soporte que AD provee para LDAP y NSPI, puede interoperar con otros servicios de directorio que los utilicen. Además se pueden desarrollar aplicaciones que utilicen LDAP para compartir informacisn de AD.

AD y DNS están integrados y comparten la misma estructura. DNS es un servicio de resolucisn de nombres y AD es un servicio de directorio.

Conóultaó fle ibleó

Los usuarios y administradores pueden utilizar el comando **Buócar** para encontrar rápidamente un objeto en la red por sus propiedades. Por ejemplo, puede buscar un usuario por su nombre, apellidos, nombre de correo electrsnico, ubicacisn de su oficina u otras propiedades de la cuenta de usuario de esa persona. La búsqueda de informacisn se optimiza al utilizar el catálogo global.

LINKS

http://www.microsoft.com/latam/technet/articulos/adbranch/default.asp



Entendiendo IPSec

IP básico no tiene seguridad. Pero, para muchas comunicaciones es indispensable. SSL resuelve el problema pero para el caso mas restringido de comunicaciones a través de Web browsing.



Si una compañía deseara conectar un Server en sus oficinas en Csrdoba con otro en su central en Bs. As. a través de Internet seguramente no permitiría que alguien snoop-eara la comunicacisn ni la modificara. Es decir buscaríamos una cone isn segura. SSL no seria la solucisn en este caso.

Otro conjunto de protocolos llamados IP Security o IPSec buscan proveer una respuesta general para seguridad en networks basados en IP . A diferencia de SSL que opera a nivel de la capa de aplicaciones (SSL es un application-layer protocol) IPSec opera en la network-layer al igual que IP. IPSec es una parte necesaria cuando se usa una cone isn VPN (Virtual Private Network) bajo el protocolo de tuneleo L2TP (Layer 2 Tuneling Protocol).

Básicamente, IPSec nos permite tomar dos computadoras y asegurar la conversacisn entre ellas con diferentes grados de seguridad. Para comprender IPSec necesitamos conocer: IPSec "actions", "filters," and "rules (acciones, filtros y reglas).

Action types de IPSec

IPSec le permite elegir cuan segura será una comunicacisn entre computadoras. Ofrece 4 niveles de seguridad (actions)

-Bloquear transmisiones
-Encriptar transmisiones
-Firmar transmisiones
-Permitir que las transmisiones viajen sin cambios. No se encripta ni se firma

E aminemos estas en más detalle: (Bloquear la transmisisn)

Esta opcisn hace lo que dice: bloquea las transmisiones. Cuando uno le dice a IPSec bloquee el trafico de maquina X a Y IPSec en Y simplemente descarta cualquier trafico que viene de X.

Esta es la opcisn de seguridad mas e trema. Si yo no quiero recibir o permitir a nadie de la subred 200.200.100.0 que me manden mail o visiten mi sitio web o se comuniquen de cualquier forma solo seteo IPSec en mi sistema descartando cualquier paquete que venga de esa subred.

(Encriptar la transmisisn: ESP)

Aquí, quiero permitir que el trafico pase de X a Y pero estoy preocupado que alguien pueda pispear (eavesdrop) la cone isn. Entonces le digo a IPSec que use un protocolo llamado: Encapsulating Security Payload (ESP) para encriptar el tráfico antes de ponerlo en la red, Los Snoopers (husmeadores) solo verán un flujo de bytes de apariencia aleatoria e ilegibles.

Notemos cuan conveniente es que IPSec funciona en la capa network de modo que puede encriptar cualquier cosa . Por ejemplo si te gusta usar telnet pero querés mejorar sobre que envía la informacisn en modo te to le decís a IPSec que cada vez que X e Y usan telnet para comunicarse que IPSec use ESP para encriptar la comunicacisn. Nada hay que modificarle a nivel de aplicaciones al servidor ni al cliente Telnet.

Ejemplo de cuando la encriptacisn seria útil. Quizás uno tenga dentro de una Intranet una maquina que maneja informacisn de importancia como sueldos o tarjetas de crédito. Supongamos que se guarda en SQL1 y es solo editada desde WS1, WS2 o WS3. Supongamos se teme que un sniffer de adentro atrape esta informacisn. Uno puede prevenir que se acceda a la base SQL con permisos. Pero no

A diferencia de SSL que opera a nivel de la capa de aplicaciones (SSL es un application-layer protocol) IPSec opera en la network-layer al igual que IP.

evitara que escuchen en la red. Con IPSec esto se puede creando una política en SQL1 que fuerce que cualquier comunicacisn hacia y desde WS1, WS2 y WS3 este encriptada. Uno debe crear políticas similares en las WS.

Otro ejemplo: supongamos tener un servidor en Csrdoba y otras oficinas en distintas ciudades del país. Supongamos que la manera de conectarnos al servidor es a través de Internet y deseamos una cone isn segura. Crearíamos una IPSec policy en el Server de Csrdoba de modo de solo aceptar trafico encriptado (nunca aceptar trafico en modo te to) Luego crearíamos políticas IPSec en las workstations de modo de solo comunicarse con el servidor en Csrdoba vía ESP.

Transmision firmada: Encabezado autenticado (AH)

En cierto tipo de ataques a redes se engaña a su computadora haciéndoles creer que transmisiones a ella provienen de alguien de confianza. Otro tipo de ataque consiste en interceptar los paquetes transmitidos, modificarlos y hacerlos continuar (lo que se llama man in the middle attack (ataque de hombre en el medio). IPSec nos deja proteger este tipo de ataque con un protocolo llamado Encabezado autenticado (AH). AH es un método de firmar digitalmente las comunicaciones. No encriptamos nuestra comunicacisn y alguien escuchando lo podría hacer. Firma digital agrega un bit de data al final de nuestros paquetes para corroborar que ellos no fueron modificados en el camino.

Transmisisn permitida

Permitido es en IPSec sin seguridad . Le dice a IPSec que deje pasar el tráfico sin cambios y sin chequeos de integridad. Es lo que nos da TCP/IP sin IPSec. ¿Para que entonces incluirlo como una accisn? De modo de poder crear reglas que restrinjan algunas cosas y no otras: bloquee todo el trafico que llega e cepto el trafico en puertos 80 y 443. Permita tráfico solo en esos puertos.

Filtros IPSec

Ahora que sabemos lo que IPSec puede hacer veamos una importante fle ibilizacisn de IPSec: sus filtros. En los ejemplos se dijo que queríamos IPSec encriptará entre dos sistemas. En otro dijimos que no solo queríamos encriptar entre 2 maquinas sino que refinara y lo hiciese SOLO CUANDO CORRE TELNET. En la seccisn de bloqueo se sugiris bloquear al web server todo tráfico desde 200.200.100.0.

Mas específicamente uno puedo usar filtros para restringir IPSec en asegurar la comunicacisn

Por IP address de la computadora fuente, el IP de la subnet o nombre DNS.

Por IP address de la computadora destino, el IP de la subnet o nombre DNS

Por puerto o tipo de puerto (port type) (TCP, UDP, ICMP, etc))

Todo esto hace IPSec muy fle ible:
IPSec Rules = IPSec Actions + IPSec Filters

Bloquear, encriptar, firmar o permitir trafico se dice es una IP action. Y acabamos de ver IPSec filtres. Para usar IPSec uno combina filtros y acciones para producir reglas (Rules). Por ejemplo si quiero

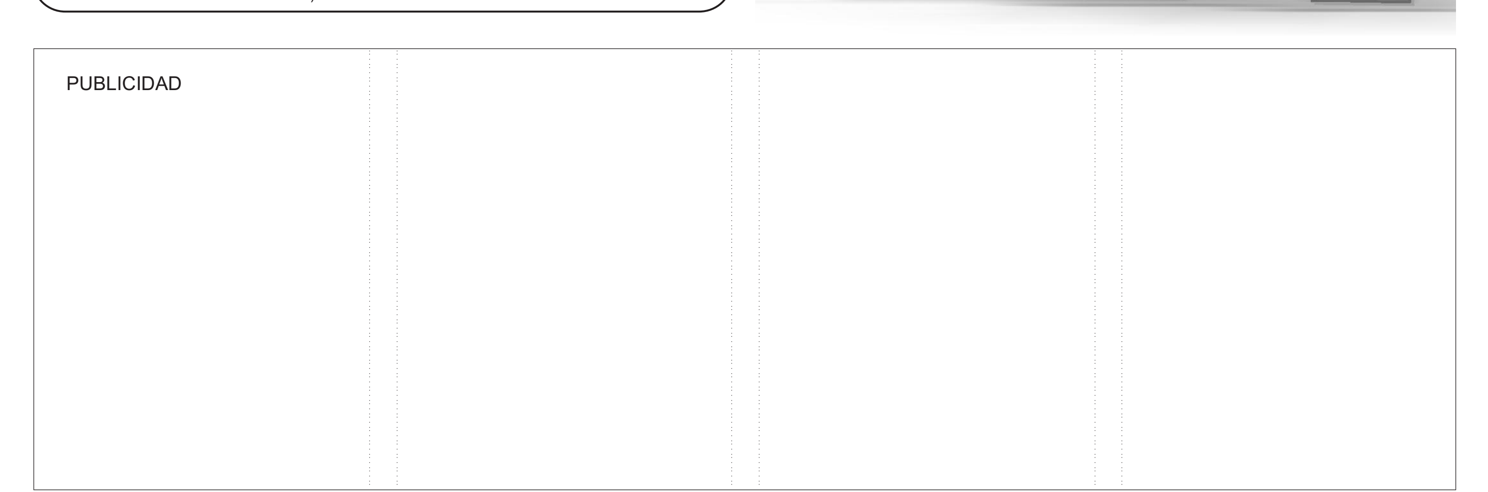
Microsoft pone en la picadora algunos exámenes

El 2 de Julio Microsoft anuncis que discontinuaría 9 e ámenes el prs imo año. Se encuentran incluidos en la lista e ámenes para Windows 98 y E change 5.0/5.5. Los siguientes e ámenes no estarán a partir del 30 de junio de 2003:

-70-056 Implementing and Supporting Web Sites Using Site Server 3.0
-70-057 Designing and Implementing Commerce Solutions with Site Srever 3.0, Commerce Edition
-70-080 Implementing and Supporting Internet E plorer 5.0 by Using the Microsoft Internet E plorer Administration Kit
-70-081 Implementing and Supporting E change Server 5.5
-70-085 Implementing and Supporting SNA Server 4.0
-70-088 Implementing and Supporting Pro y Server 2.0
-70-091 Designing and Implementing with Office 2000 and Visual Basic for Applications
-70-098 Implementing and Supporting Windows 98
-70-105 Designing and Implementing Collaborative Solutions with Outlook 2000 and E change Server 5.5

Microsoft informs que a pesar que los e ámenes serían retirados el año entrante, cualquier certificacisn obtenida con estos e ámenes seguirá siendo valida.

Microsoft normalmente limita la comunicacisn de las discontinuidades de los e ámenes una vez al año, normalmente en Junio. (Vea "Discontinuation of E ams" en la página Web de Microsoft MCP en www.microsoft.com/traincert/.)



decirle a IPSec en una dada computadora: encripte todo el trafico bajo telnet de la computadora en 10.10.11.3 . Esa es una Regla (Rule). Tiene una parte filtro y una accisn:

El filtro dice: solo active esta regla si hay trafico que es (1) de la direccisn IP 10.10.11.3, y (2) cuando use puerto 23 (telnet usa puerto 23)

La parte de la accisn dice: encripte ese trafico .

Windows 2000, XP o .NET server implementan IPSec construyendo políticas. Las políticas están hechas de una o mas reglas. Y, reglas están hechas de filtros (¿Lo debo hacer?) y acciones (¿que debo hacer?).

Firmado y encriptado necesitan una pieza mas: autenticacisn

En orden de poder hacer funcionar firmado digital o encriptacisn se necesita establecer keys (llaves) (básicamente password). Así, que cuando uno crea una regla IPSec debe decirle a IPSec como autenticarse.

La implementacisn de IPSec de MS tiene algo con poco sentido: e ige autenticacisn ya sea que IPSec lo necesite o no. Si uno permite tráfico sin cambiarlo o lo bloquea totalmente en principio no necesita establecer llaves pre-acordadas. Así que en teoría cualquier regla que solo incluya permitir y bloquear no debería requerir ningún método de autenticacisn. Pero, MS nos lo pide de todos modos aun cuando no se usa. Así que si estable una regla que solo bloquee y/o permita elija cualquier método de autenticacisn ya que da lo mismo.

Y cuando usaríamos solo permitir o bloquear'. Cuando uno setea IPSec a realizar una de sus habilidades más interesantes: por ejemplo construir filtros de paquetes muy fle ibles.

Como hacemos para activar todo esto. IPSec se maneja por políticas: locales o basadas en el dominio. Uno crea reglas IPSec del Local Security Policy program (secpol.msc) or via Group Policies. Las políticas contendrán una o mas reglas. La mejor estrategia para crear las reglas es

El Ipsec de MS soporta 3 métodos de autenticacisn: Kerberos, certificados o una llave-concertada (agreed-upon key).

El IPSec de MS soporta 3 métodos de autenticacisn: Kerberos, certificados o una llave-concertada (agreed-upon key). Kerberos solo funciona entre computadoras que están en un dominio Active Directory (AD) o en Active Directories que se confían mutuamente. Simplemente tener dos computadoras que tengan clientes Kerberos no será suficiente y aun tener 2 sistemas Windows miembros del mismo realm Kerberos (Uni -based Kerberos versisn 5 realm) no basta. Quizás MS debería haber llamado a esta opcisn Active Directory .

La opcisn certificados le permite usar la PKI (Infraestructura de llaves publicas) para identificar una maquina. La opcisn preshared key (llave pre-acordada) permite usar un string de te to como llave. No muy seguro. Esta opcisn es muy buena para e perimentar. No hay necesidad de establecer certificados o un dominio AD. Solo basta decirle a ambas maquinas usar preshared key y escribir cualquier te to como esto es un secreto en las maquinas. No seria muy útil en produccisn pero si para enseñanza.

definir filtros y acciones primero y luego pegarlas para armar las reglas.

Para empezar, abra Local Security Policy (Start/Programs/Administrative Tools/Local Security Policy) y mire la carpeta labelled "IP Security Policies on Local Machine."

Botsn-derecho en ese folder y elija "Manage IP filter lists and filter actions," y cree los filtros y acciones deseadas.

Cierre los diálogos y haga botsn-derecho esta vez sobre "Create IP Security Policy" para crear una política.

Una vez que tiene la política como desea haga botsn-derecho y asígnela (assign). Ud vera que MS ha pre-creado 3 políticas. Solo una puede estar activa. Así, que si no la asigna no vera su efecto.

Para leer un ejemplo paso a paso del uso de IPSec (para encriptar la comunicacisn entre 2 maquinas) vea el MS Q article Q301284.

L I N K S

http://support.microsoft.com/support/kb/articles/Q301/2/84.ASP

Espacio Ne

Historia de 2 grietas de seguridad

En forma reciente se han reportado 2 muy importantes flaws (grietas), una con pgp, el programa de fuente abierta de encriptacisn de e-mail (alguien puede desencriptar y leer su e mail encriptado) y otro en la implementacisn de Microsoft de chequeos de certificados en cadena en SSL, el protocolo usado para asegurar las transacciones comerciales en Internet (alguien podría utilizar ilegalmente (spoof) la direccisn IP de un sitio Web protegido por SSL y por ende obtener su número de tarjeta de crédito).

Como no es mi pretensisn minimizar la seriedad de las grietas, y considerando que no cuento con el conocimiento de todos los hechos, mi interés principal radica en la forma en que las grietas fueron reportadas y en la respuesta dada a los reportes. Mucho ha sido dicho sobre la vulnerabilidad de los productos Microsoft y poco sobre la de otros productos. Recientemente esto ha ido cambiando con todo tipo de compañías haciendo correr su propia lista de vulnerabilidades y parches (patchs), con un foco más equitativo en grietas de cualquier producto. Aquí tenemos una oportunidad de contrastar la respuesta al reporte de la vulnerabilidad de Microsoft y la de un producto de fuente abierta, lo que yo encuentro interesante sobre esas 2 vulnerabilidades y lo que se de ellas.

investigadores que colaboraban con Bruce Schreiner en la investigacisn del problema. Los investigadores actuaron con responsabilidad, aparentemente dándole tiempo a algunos proveedores de PGP para arreglar la grieta, y la oportunidad de que otros investigadores contestaran el reporte después de una adecuada investigacisn (a la vez de proveer a los usuarios una forma de evitar ser victimizado)

La respuesta de la comunidad de seguridad a la grieta fue interesante, dijeron que para e plotar la grieta, los usuarios no deberían usar la compresisn (si, claro, los usuarios nunca hacen eso) y además responderle al remitente del mensaje encriptado dañado. El remitente es el hacker que capturs el mensaje y lo modifics, el usuario es quien recibe los datos basura.

Pienso que todos debemos asumir que nada es perfecto y que estamos e puestos a un riesgo mucho mayor del que creemos. No hay un lugar donde esconderse y todavía seguir haciendo una vida normal. Como si fuéramos recién llegados a una tierra e traña, debemos unirnos y seguir encontrando y tapando agujeros, independientemente del origen. Sería destructivo no hacerlo así.

En Microsoft y SSL:

Es interesante que el investigador ni siquiera se preocupara por contactar a Microsoft. Redmond tiene una larga historia de respuestas a grietas identificadas, como se demuestra por todos los boletines de seguridad con links gratuitos a las correcciones.

Por otro lado la respuesta pública de Microsoft trata de minimizar la grieta del SSL diciendo que es muy difícil hacer spoof de un sitio Web. Y no lo es. Encriptacisn aparte, nosotros usamos el SSL para autenticar el servidor, si eso se va, a quien le importa si los datos fueron encriptados, pero al servidor equivocado.

Y todo esto recibe más atencisn de los medios que la débil proteccisn de la base de datos de números de tarjeta de crédito de muchos sitios de comercio electrsnico. ¿Porqué hacer spoof de un sitio de la red con el propssito de capturar un manojo de números de tarjetas de crédito antes de ser descubierto cuando es posible hackear y robar números de tarjetas de crédito de a miles, o comprarlas? ésta vulnerabilidad, al contrario que la de Microsoft, se encuentra allí afuera con muchos casos documentados de e plotacisn e itosa.

En PGP:

La grieta en PGP fue descubierta por

Cuando el usuario responde aportando una copia del mensaje dañado para preguntar al remitente sobre él, el mensaje puede ser desencriptado por el hacker. Y como todos sabemos los usuarios nunca podría contestar e incluir una copia de lo que se le mands ¿no es cierto?

En ambos:

Es interesante que ambas grietas representen tspicos de ingeniería y no errores de programacisn. También demuestra que tanto los recursos de fuente abierta y los programas propietarios pueden tener grietas, y que los defensores de ambos desean e presar a viva voz cuán duro es e plotarlas.

Apuesto a que habrá muchas respuestas a esta columna que afirmen que la respuesta de la fuente abierta es más profesional. Estoy de acuerdo, el investigador que descubris la grieta acudis a otros investigadores para que la confirmen, para entonces publicaron los detalles juntamente con las recomendaciones para arreglarlo y sobrellevarlo. El descubrimiento de la grieta de Microsoft fue directamente a la prensa.

(Artículo e traído del Newsletter de MCP Magazine del 19/8/ 2002.- Security Watch http://mcpmag.com /security/) *por* ***Roberta Bragg***



DNS en W2k, un cambio



Para Windows NT, DNS era una herramienta secundaria, estaba ahí para que la utilizaran los programas que accedían a Internet (buscando servidores de correo y páginas Web), mientras que WINS se encargaba de resolver las ubicaciones de los Domain Controllers, servidores y estaciones de trabajo, es decir el soporte al funcionamiento de la red estaba en sus manos.

Hasta Windows NT el protocolo por defecto era NetBeui pero en Windows 2000 es reemplazado en esa tarea por TCP/IP. Debido a eso el resolutor de nombres principal deja de ser WINS, que es reemplazado por DNS. Incluso, si instalamos Active Directory (uno de los mayores avances en Win2k sobre NT), estamos obligados a instalar DNS, porque sin él, AD no funciona.

Al ser tan necesario, en Microsoft se han esmerado para mejorar su funcionalidad. Si bien DNS en NT 4.0 era fácil de configurar y confiable, al DNS de Win2k se lo hizo compatible con los RFC 2136 y RFC 2052 (Request For Comments - Solicitud de comentario: las normalizaciones en Internet llevan esos nombres), lo que quiere decir que ahora soporta actualizaciones dinámicas, permitiendo automatizar el proceso de añadir informacisn sobre nuevas máquinas a la base de datos DNS y aumenta los tipos de informacisn que puede administrar. Por ejemplo, un servidor DNS que no cumpla con la RFC 2052 podía decirnos que máquinas actuaban como servidores en un dominio dado, pero no cuales eran servidores Web o FTP. Active directory cumple con la RFC 2052 para que DNS ayude a las estaciones de trabajo a encontrar controladores de dominio y otros servidores específicos de AD.

WINS: Duro de matar

Está bien, dejs de ser el jefe en la resolucisn de nombres para Win2k, pero mientras e istan máquinas con versiones anteriores de Windows instaladas en ellas y conectadas a una red, aunque estén controladas por Win2k, vamos a seguir necesitando resolver nombres NetBIOS (los que usa NetBeui).

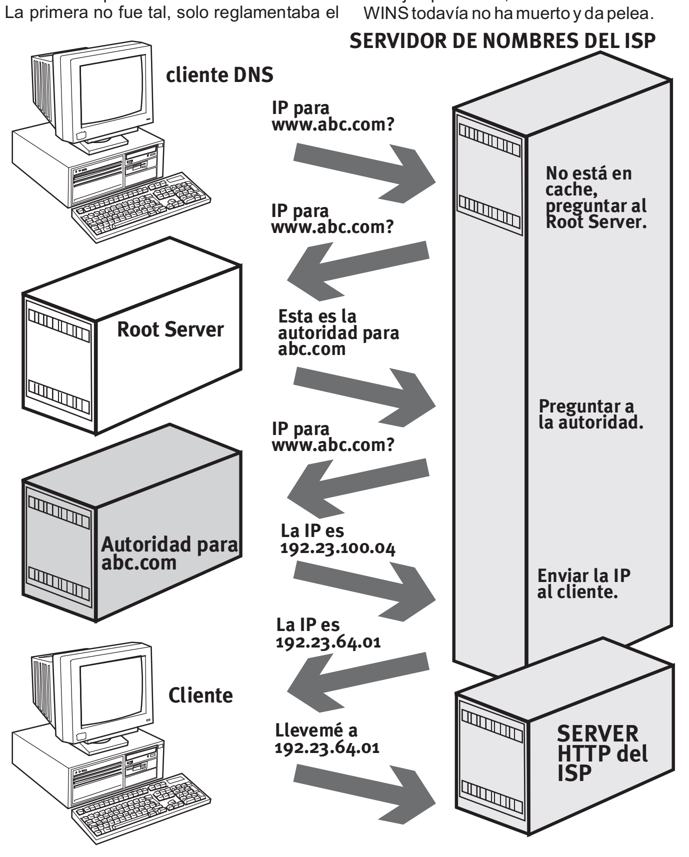
Vamos a tratar de aclarar un poco las cosas: Las aplicaciones que acceden a recursos en una red se comunican con los protocolos de red a través de APIs (Application Program Interface - Interfaz de programa de aplicacisn). Desde 1985 Microsoft construys sus aplicaciones sobre una API (desarrollada también por Microsoft) llamada NetBIOS (Network Basic Input/Output - Entrada/Salida Básica de Red). El resto del mundo Internet, por el otro lado, sslo usa una API diferente: Sockets. La versisn PC de sockets se llama Winsock, esto quiere decir que Windows utilizs durante varios años las 2 API, y recién en las versiones Win2k decidis inclinarse por la que prefería el mundo aunque no fuera la que Microsoft desarrolls, es decir que eligis Winsock. Pero el problema es que hay toda una pléyade de aplicaciones dando vueltas por ahí tratando de acceder a la red utilizando NetBIOS. Por lo tanto NetBIOS sobre TCP/IP (llamado NetBT o NBT) es fundamental para que los sistemas operativos y aplicaciones más viejas sigan funcionando en las redes nuevas. Los problemas siguen, el viejo NetBIOS resolvía nombres simplemente haciendo broadcasting, lo cual va a ser inconveniente en cualquier red ruteada (los mensajes broadcast no son retransmitidos por los routers), si la máquina cuyo nombre se está buscando está en algún segmento de la red mas allá del router, directamente no será encontrado. Por supuesto que hubo gente que nots esto antes que nosotros, lo que nos lleva a otros 2 RFCs, el 1001 y el 1002.

Los RFCs dieron opciones para solucionar el problema:

La primera no fue tal, solo reglamentaba el uso de broadcasts.

La segunda, era crear alguna clase de servidor de nombres y usarlo. Entonces, cuando un cliente necesitaba resolver un nombre, todo lo que debía hacer era mandar un mensaje punto a punto al servidor de nombres y esperar su respuesta; el nombre genérico es NBNS (NetBIOS Name Server - Servidor de Nombres NetBIOS), y el nombre del NBNS mas usado es WINS (Windows Internet Name Server - Servidor de Nombres Windows para Internet).

Recuerde que para no necesitar WINS, no solamente TODAS las computadoras deben trabajar con Win2k, sino que además TODOS los programas que utilicen la red deben estar basados en winsock y no en NetBIOS. Así, aunque ahora DNS tiene mas trabajo que antes, en las redes Windows, WINS todavía no ha muerto y da pelea.



Filosofía de DNS: Control local, acceso mundial

DNS está ahí para resolver nombres a direcciones IP, que son las que realmente comprende y puede manejar el protocolo TCP/IP. Casi todos (si no es que todos) los sitios que uno puede encontrar en Internet tienen un nombre amigable (www.ne web.com.ar) asociado con una direccisn IP (100.200.300.400), y también e iste una autoridad en Internet (La interNIC, de la que hablaremos en otra nota), así que porque no dejamos que ésta autoridad mantenga una base de datos centralizada que nos diga que direccisn tiene cada nombre asignado en la red.

Bueno, no lo hacemos por la sencilla razsn de que hoy debe haber apro imadamente 200.000.000 de computadoras conectadas a Internet, y la base de datos tendría unos 8 GB de informacisn, por eso éste Servidor Global de Nombres (SGN) estaría bastante ocupado. Además, sería fatal que cada vez que alguien quiera agregar una máquina o cambiar un nombre en su red, debiera enviar un mensaje a los ocupados muchachos del SGN y esperar la confirmacisn de que realizaron el cambio en las bases. Por último, desvirtuaría la filosofía de Internet: Descentralizacisn (Internet nacis de ARPA Net, un proyecto del departamento de defensa de EEUU en el cual, si una parte de la red se rompía por un ataque, el resto debería poder seguir trabajando).

Entonces no, no vamos a tener un Servidor Global de Nombres y en cambio lo que tenemos son unas reglas para hacer funcionar la resolucisn de nombres en forma distribuida a lo largo de las redes:

Cada organizacisn instala y mantiene sus propios servidores DNS, los cuales referencian sslo las máquinas que pertenecen a su organizacisn. Es responsabilidad del propietario de cada subred que sus servidores DNS funcionen y lo hagan bien. Si necesito acceder a www.ibm.com, entonces IBM es quien debe mantener servidores DNS que le digan a mi browser a que direccisn IP se debe dirigir.

La interNIC mantiene referencias solo a los servidores DNS de los dominios registrados. Es decir que la interNIC NO puede darme la direccisn de www.ibm.com, pero puede decirme que IBM tiene 6 servidores DNS que pueden resolver ese nombre y, por supuesto, puede darme las direcciones de esos servidores. No hay ninguna magia en eso, ya sabemos que la interNIC es el grupo que registra los nombres de dominio en Internet, y se niega a registrar un nuevo dominio si no se le

proveen por lo menos 2 direcciones de servidores DNS que resuelvan los nombres de dicho dominio.

El software de servidores DNS es lo suficientemente inteligente como para preguntarle a otros DNS, cuando no puede resolver el nombre por si solo. Es una de las cosas que hace que todo esto funcione: si alguien dentro del dominio www.ibm.com trata de acceder a www.microsoft.com, el primer DNS con el que se encontrará la solicitud será uno de los DNS de IBM. Como ese servidor no podrá resolver el nombre se conectará con los servidores de la interNIC, los que le darán la direccisn de los DNS de Microsoft, con esa informacisn en la mano, el DNS de IBM que se está encargando de ésta sesisn, se comunica con el DNS de Microsoft para que éste último le diga cual es la direccisn de la máquina llamada WWW dentro del dominio microsoft.com Pero ahí no termina el proceso, todavía falta que el DNS de IBM le entregue esa direccisn al browser que había pedido la comunicacisn para que, ahora si, el browser emita un mensaje a la direccisn de www.microsoft.com. Esto, por supuesto, sucede a velocidades suficientemente altas como para que no nos decidamos a aprender las direcciones IP por nosotros mismos.

Tolerancia a Fallos

Esta es la e plicacisn de porqué la interNIC, pide 2 servidores DNS para registrar un dominio. Cada dominio tiene uno y solo un Primary DNS (DNS primario), el cual se setea de esa manera. Además todos los dominios registrados, y todos aquellos que desean tener una cuota de fault tolerance (tolerancia a fallos) tienen algún número de servidores DNS secundarios, los cuales contactan al primario cada cierta cantidad de tiempo y copian su base de datos. Simplemente tienen un backup de la base del DNS primario y pueden satisfacer resoluciones de nombres cuando el DNS primario está muy ocupado o caído.

qonas, Dominios y Delegacisn

Estrictamente hablando, los servidores DNS no guardan informacisn de nombres por Dominio, sino que lo hacen por qonas. Una zona es el rango de direcciones IP de las cuales se ocupa un servidor DNS determinado . En principio es solo una cuestisn de nombres y la qona puede coincidir con el Dominio. Pero si una compañía crece, se fusiona o adquiere otra puede resultar que mantener una sola qona para todo el Dominio no sea la opcisn mas apropiada. Pro ejemplo si la empresa acme cuyo dominio es acme.com, instalada en Bs. As. mueve todo su departamento de fabricacisn de juguetes a una provincia donde le sea mas barato fabricarlos (por ej.: Santa Cruz), puede ser que le sea conveniente crear un subdominio (que todavía es parte del domino acme.com) llamado juguetes.acme.com. Como los dos centros estarán separados por cientos de kilsmetros. La opcisn de que un DNS se encargue de todas las resoluciones será costosa en consumo del ancho de banda de la comunicacisn desde Santa Cruz hasta Bs.As. para resolver el nombre de una máquina que posiblemente está al lado de la que inicis la peticisn. Lo que se puede hacer en es caso es Delegar la autoridad para la resolucisn de nombres del subdominio juguetes.acme.com a un servidor DNS instalado en la sede de Santa Cruz. Entonces 2 servidores DNS que pertenecen al mismo dominio padre (acme.com) atienden solicitudes de 2 qonas distintas a través del proceso de Delegacisn.

Al revés

Hasta acá vimos la tarea principal de los DNS qué es convertir nombres a direcciones IP, lo que se llama forward name resolution (resolucisn de nombres directa), pero DNS puede hacer la tarea inversa: responder cuál es el nombre de dominio asociado a una direccisn IP determinada, y esto se llama reverse name resolution (resolucisn de nombres inversa).

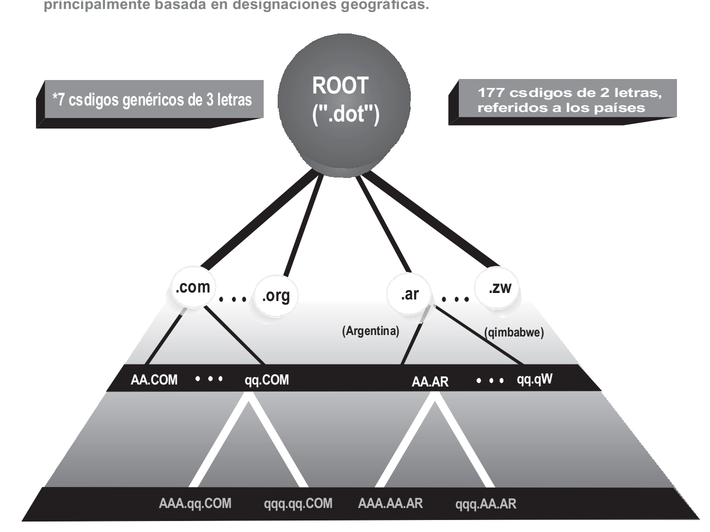
Los DNS almacenan la informacisn para encontrar nombres de dominio en archivos llamados zone files (archivos de zona). Pero para cada subnet de Internet hay una zona llamada reverse lookup zone (zona de búsqueda inversa). El nombre de esos archivos es raro, para construirlo se toma la direccisn de la red (205.22.42.0/8 por ejemplo), se descartan los octetos que identifican los hosts (en éste caso los últimos 8 bits), se invierten los que referencian a la red (en éste caso pasamos de 205.22.42 a 42.22.205) y se le agrega .in-addr.arpa . Con lo cual para un DNS que sea la autoridad de una zona correspondiente a un dominio que tenga asignada la direccisn 205.22.42.0/8, el nombre del archivo de su reverse lookup zone es 42.22.205.in-addr.arpa y ese es el lugar en donde el DNS buscará la respuesta a consultas del tipo ¿csmo se llama el hosts cuya direccisn es 205.22.42.37?

De ésta manera llegamos al final de la presentacisn de los servicios DNS. Ahora podemos pasar a poner manos a la obra con una instalacisn básica de un DNS bajo Windows 2000.

LINKS

http://###www.microsoft.com/latam/technet/articulos/adbranch/default.asp

Estructura jerárquica de DNS (Domain Names System)



Exámenes de Seguridad bajo desarrollo

El 30 de Junio, Microsoft publics informacisn sobre el desarrollo de un nuevo e amen basado en Seguridad. Según la guía de objetivos del e amen publicada en www.microsoft.com/traincert/e ams/70-214.asp. EL e amen 70-214, Implementing and Administering Security in a Windows 2000 Network , es un MCA y MCSE electivo cuya beta se espera sea lanzada en Noviembre.

El e amen es la continuacisn de los comentarios que el grupo de capacitacisn y certificacisn de Microsoft hizo más temprano este año considerando el posible desarrollo de una certificacisn de seguridad.

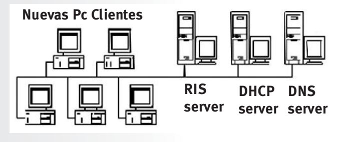
En otra noticia relacionada a certificaciones, Dan Trua , director del grupo de certificacisn de habilidades y valoracisn de estrategias (Microsoft's certification skills and assessment-strategy group), dijo que es improbable que Microsoft agregue elementos de laboratorio a las pruebas de certificacisn, Nosotros no tenemos planes específicos para lanzar e ámenes de laboratorio, aunque continuamos e plorando innovaciones en los e ámenes dijo Trua .

Él dijo que Microsoft ha tenido é ito con simulaciones dentro de los e ámenes, y "nosotros continuaremos nuestro gran énfasis en eso . Él también mencions la posibilidad de tener más interaccisn del producto dentro de las pruebas.

Preguntas para e amen Microsoft 70-210

Usted debe instalar Microsoft Windows 2000 Professional en un conjunto de nuevas maquinas. Todas las PC cumplen con la norma PXE. Usted instala un servidor RIS, un DHCP y un servidor DNS.

Sin embargo la instalacisn automática falla. La red está distribuida como muestra la figura:



¿Cuál es la causa más probable del fallo de la instalacisn automática?

a)Un problema de cableado de red.

b) No está funcionando Active Directory.

c) está mal configurado el DHCP.

d) Lo más probable es que las PC no sean realmente PXE.

Respuesta:
La opcisn correcta es la b. Para que una instalacisn automática funcione, todo el proceso debe realizarse sobre la estructura de un Active Directory. Las respuestas que contradicen los enunciados son siempre una trampa.



PRESENTANDO IDS

Cuando se habla de seguridad en redes, por lo general se asocia la tecnología de seguridad con mecanismos de control de acceso como los firewalls, servidores Pro y y ACL (Access Control Lists - Listas de Control de acceso) de routers. Todos ellos están diseñados para restringir el flujo de tránsito hacia y desde las redes privadas, en un intento por preservarlas del acceso de atacantes desde Internet.

Sin embargo incluso el mejor de los dispositivos de filtrado fallará en su misisn de proteger la red si los recursos accesibles desde Internet son vulnerables a ataques. Individuos maliciosos pueden utilizar los canales de comunicacisn abiertos (HTTP, FTP, e-mail, DNS) para comprometer, en forma remota, la seguridad de un sistema dentro de una red, y entonces usar ese sistema atacado, como base para atacar otros sistemas dentro de la red. Muchas infraestructuras de red se han vuelto tan complejas y dispersas que los administradores de la red pueden llegar a tardar varios días en enterarse de un defacement (cambio de cara) de su página Web. En un caso particular, un sysadmin tuvo conocimiento de que su página Web había sido atacada después de que un usuario le avisara a la oficina de relaciones públicas de la empresa. La gente de relaciones pública se lo dijera a un gerente quien se lo dijo al administrador de la red.

En términos amplios, los IDS son tecnologías que intentan dar soporte a los procesos de deteccisn de intrusos

Realmente, no la mejor manera de enterarse de una cosa así. Ahora la buena noticia es que los IDS (Intrusion Detection Systems - Sistemas de Deteccisn de Intrusos) están alcanzando un nivel de madurez que les permite llenar el hueco en la seguridad, proveyendo una manera de monitorear la red para detectar el mal uso de la misma y "e ploits" activos. Los IDS pueden ser host-based (basados en una computadora) o network-based (basados en la red).

Que es un IDS?

La ID (Intrusion Detection - Deteccisn de Intrusos) es un proceso de seguridad diseñado para monitorear y analizar eventos en sistemas y redes para detectar un posible mal uso o accesos no autorizados. En términos amplios, los IDS son tecnologías que intentan dar soporte a los procesos de deteccisn de intrusos. Además pueden dividirse en varias subcategorías: IDS embebido, honeypots (tramperas), chequeadores de integridad de archivos e incluso scanners antivirus. Nuevos conceptos y términos están relacionados con éste campo, dado el progreso de la tecnología y al intento de los desarrolladores de introducir nuevas funcionalidades y de diferenciar sus productos de los de la competencia, aprovechando el crecimiento de éste espacio. Las compañías están empezando a construir conceptos como "protocol anomaly detection" (deteccisn de anomalía en el protocolo), "distributed IDS event correlation" (correlacisn de eventos distribuidos de IDS); y la mayoría de los productos en uso actualmente son clasificados como "pattern matching systems" (sistemas de búsqueda de patrones). IDS es similar a un detector de movimiento instalado en una casa. Cuando las rejas y cerraduras fallaron en su tarea de mantener afuera a los intrusos, el censor puede detectar movimiento en el interior de la casa y disparar una alarma. Por supuesto que es importante ubicar correctamente el censor. Si se lo pone en el último rincsn del garaje, no será capaz de detectar intrusos ingresando por la ventana de la cocina.

Network Intrusion Detection Systems

Los NIDS monitorean el tráfico de la red. Usualmente están basados en dos principios: pattern-matching (reconocimiento de patrones) y deteccisn de anomalías por estadísticas o mediante el uso de algoritmos. El reconocimiento de patrones trata de identificar secuencias específicas de atributos (signatures - *firmas*) dentro de los paquetes. Puede ser una direccisn IP origen, destino, o ciertos caracteres en los encabezados o los datos. La deteccisn estadística o algorítmica de anomalías en los protocolos identifica el tráfico que cumple con determinadas características, por ejemplo la cantidad de paquetes SYN (los paquetes que intentan iniciar una sesisn) recibidos por minuto o la cantidad de cone iones intentadas en un período de tiempo determinado. En los términos de NIDS, los patrones usualmente son denominados signatures (firmas) y las reglas estadísticas o algorítmicas utilizadas para detectar las signatures son llamadas reglas . Por ejemplo el gusano csdigo rojo puede ser identificado dentro del tráfico de la red como un paquete dirigido al puerto 80 (protocolo HTTP) que contiene la siguiente firma (o patrsn o signature) dentro del sector de datos:

GET /default.ida? XXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX%u90 90%u6858%

(Simplificado para la publicacisn)

También se pueden detectar intentos no autorizados de logueo o ataques de fuerza bruta. Esto se lograría reportando (a través de una regla NIDS), por ejemplo cuando suceden mas de 20 intentos fallidos de logueo por minuto. Los NIDS más modernos pueden ser configurados para reportar casi cualquier clase de anomalía hipotética. Es importante mencionar que muchos productos NIDS permiten a los administradores del sistema definir nuevas firmas y reglas. Sin embargo, NIDS no sslo puede ser utilizado para detectar ataques activos, sino también para rastrear problemas en la red, o para pescar paquetes que pueden ser interesantes para el staff de networking.

Por supuesto que la habilidad de un IDS para hacer su trabajo implica que el sensor es capaz de hacer sniffing (olfatear - capturar y revisar los paquetes que circulan por una red) de todo el tráfico desde y hacia los sistemas monitoreados y comparando todos los paquetes con la base de datos de *firmas* maliciosas. Este hecho hace necesaria la instalacisn del NIDS en un segmento de red que le permita capturar TODO el tráfico a monitorear. Esto se puede lograr instalando puertos espejados en los switches, o instalando hubs en las cone iones uplink de las interfaces de los routers o switches. En una red de arquitectura redundante, cada link redundante debe contar con su propio NIDS. Se debe evitar crear puntos de falla sin respaldo cuando se diseña una solucisn de IDS.

Los estudios demuestran que la mayoría de los ataques ocurren en las redes internas, por eso se debe considerar seriamente la implementacisn de IDS, no solo en la DMq (DeMilitarized qone - qona DesMilitarizada - la porcisn de la red donde se permite acceso público, como el ftp server, Web server) sino también en la red interna. El mayor desafío en la monitorizacisn de actividad maliciosa en la red interna es que puede provenir de accesos autorizados, es decir usuarios registrados en el sistema, que no necesariamente utilicen técnicas de hackeo

Los estudios demuestran que la mayoría de los ataques ocurren en las redes internas, por eso se debe considerar seriamente la implementacisn de IDS, no solo en la DMq sino también en la red interna

reportables por el IDS. La respuesta a dicho desafío es usar una combinacisn de NIDS y HIDS (Host-based IDS - Sistema de Deteccisn de Intrusiones basado en computadoras).

Host-based Intrusisn Detection

Los HIDS (Host-based Intrusion Detection Systems) están diseñados para detectar eventos dentro de un host, csmo por ejemplo, el uso del comando "run as" o accesos legítimos a documentos confidenciales, pero realizados a horas desusadas, lo que puede significar la presencia de un intruso. Los mecanismos de HIDS van desde un sistema básico de auditoria hasta métodos de deteccisn avanzados, y han demostrado ser más eficientes para detectar un potencial mal uso de los sistemas desde adentro de la red local. Algunos productos incorporan los dos sistemas, consolidando la salida de reportes a una única consola.

IDS no es una cura milagrosa

La encriptacisn, diseñada para evitar el acceso no autorizado a la informacisn, es particularmente problemática para los sistemas de deteccisn de intrusiones. Protocolos que son ampliamente utilizados csmo SSL (Secure Sockets Layer - Capa de Cone iones Segura), SSH (Secure Shell - Intérprete de comandos Seguro) o IPSec (IP Seguro) utilizado en las VPN (Virtual Private Networks - Redes Privadas Virtuales), evitan que los NIDS puedan inspeccionar el tráfico para compararlo contra las *firmas* de los ataques conocidos. Los payloads (datos dentro de los paquetes) encriptados convierten a éstos protocolos en e celentes vehículos para que un atacante pueda evadir la deteccisn por parte de un IDS.

Otra limitacisn importante es la velocidad de la red. Limitaciones de hardware y algoritmos de comparacisn ineficientes, imponen una limitacisn al número de paquetes que se pueden capturar y analizar dentro de un período de tiempo determinado. Una vez que éste límite es alcanzado, los IDS comienzan a "perder " paquetes (ignorar el tráfico). Pocos NIDS actualmente disponibles en el mercado pueden trabajar en redes "gigabit".

Para hacer más fácil la tarea de los hackers han aparecido herramientas que burlan los sensores de los IDS. Algunas de ellas (por ej.: stick) bombardean al NIDS con bases de datos de *firmas* de ataques, haciendo que algunos IDS desborden de falsos mensajes de alerta. Las organizaciones deben comprender claramente los riesgos que encierran herramientas como esa, usados contra los NIDS y csmo responder a esas alertas. Usualmente los atacantes tratarán de evadir la deteccisn de los NIDS con la finalidad de poder realizar ataques verdaderos y hacerlos difíciles de detectar.

Utilizar un NIDS, esperando obtener altos grados de efectividad incluye una gran cantidad de mantenimiento. No se puede sencillamente instalar el software de NIDS y dejarlo funcionar desatendido. Nuevas *firmas*, cambios en la red, nuevo software, todos esos eventos requerirán un afinado en el NIDS. Para alcanzar la má ima efectividad, las *firmas* deben ser frecuentemente actualizadas, los límites deben ser ajustados para evitar falsas alarmas y los administradores deben monitorear los registros de eventos para conocer el comportamiento normal de la red en su propio entorno y poder diferenciarlo de comportamientos e traños. Los procesos de agregar o quitar elementos y servers en la red deben ser acompañados por nuevos ajustes en los NIDS. No hacerlo así puede resultar en la pérdida de confiabilidad en el sistema. Estas actividades pueden consumir muchos recursos, es por eso que (en USA por ejemplo) están surgiendo compañías que se dedican e clusivamente a hacerse cargo de la administracisn de los NIDS de las empresas que tercerizan esa tarea.

Los NIDS también pueden ser configurados para administrar el tráfico de manera proactiva, por su cuenta o interactuando con otros productos, firewalls u otros componentes de la red, en respuesta a los eventos. Pro ejemplo, algunos NIDS pueden resetear sesiones TCP (enviando un paquete RST al origen) basándose en la ocurrencia de triggers (disparadores) específicos. Algunos pueden integrarse con otro software de administracisn y provocar una reconfiguracisn automática de la red.

¿Se puede confiar en ellos?

La mayoría de los e pertos de la industria coinciden en que los IDS todavía no han alcanzado la madurez, total. No se ha llegado al punto en que se pueda confiar ciegamente en que la reconfiguracisn automática que el software decida, sea la solucisn. El mayor problema con las respuestas automáticas a los eventos sobre la red es que el IDS en sí, se convierte en una amenaza potencial. Si un atacante se da cuenta de que el NIDS cierra el puerto 80 para la direccisn de origen desde donde



proviene el ataque, fácilmente puede averiguar direcciones de clientes y socios de la empresa que tiene implementado el NIDS, y realizar ataques mediante spoofing de esas direcciones, lo que produciría un DoS (Denial of Service - Negacisn de Servicio) a usuarios legítimos.

Otra complicacisn proviene de la arquitectura de los IDS. En muchos casos, la implementacisn requiere comunicacisn entre agentes (traffic snifing devices - dispositivos de captura de tráfico) y administradores (los dispositivos que gobiernan la distribucisn de políticas y la manera de procesar las alertas entre las estaciones de administracisn y las consolas). Para ello se deben configurar direcciones IP trusted (confiables) desde la DMq (DeMilitarized qone - qona DesMilitarizada) o, peor aún, desde Internet, para que se les permita el acceso a la estacisn de administracisn de la red. Si no se hace un análisis profundo y concienzudo de dicha configuracisn, la implementacisn del NIDS puede provocar un daño enorme. En algunos casos se debería crear una red de administracisn diferente para usar interfaces de red separadas en las máquinas agente.

Para finalizar, la siguiente es una lista de las tareas que generalmente puede realizar un Network Intrusisn Detection System:

-Análisis casi en tiempo real del tráfico, en búsqueda de *firmas* de ataques conocidos.

-Deteccisn y reporte casi en tiempo real de anomalías en el tráfico de la red.

-Alerta del personal administrativo cuando se detecta un ataque potencial.

-Ejecucisn de una accisn correctiva, previamente definida.

-Análisis y reporte sofisticado (no en tiempo real).

LINKS

http://www.snort.org/ ,

http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm

Los NIDS también pueden ser configurados para administrar el tráfico de manera proactiva, por su cuenta o interactuando con otros productos

LOS CUATRO PASOS

Consejos para iniciar el camino de la seguridad informática

Es tiempo de que lo urgente le de espacio a lo importante. Las redes de computadoras han estado creciendo, interconectándose y, sobre todo, abriendo sus puertas a Internet.

Si la humanidad no tuviera secretos (o no tuviera curiosidad) el solo hecho de conectarnos nos solucionaría las necesidades de comunicacisn, pero la realidad es otra. Lo cierto es que una vez que nos interconectamos, estamos abriendo una puerta por la que pueden salir cosas que deberían quedar adentro o entrar personas que nos gustaría que permanecieran afuera. Alguien tiene que cuidar esa puerta. ¿Quién será esa persona?, pues el encargado de seguridad de la red.

Pero ¿que pasa?, ésta es un área que se ha descuidado y en el país no hay mucha gente que tenga conocimiento profundo del tema. Es, entonces, una buena oportunidad para ocupar un espacio, todavía poco e plotado. ¿Qué hacer?, csmo sugerencia permítanos sugerirle éstos cuatro primeros pasos.

Paso Uno: Ver las opciones

El primer paso debería consistir en determinar e actamente que significa para usted seguridad . ¿Se quiere especializar en algunos aspectos técnicos de la seguridad?, digamos establecer y configurar los firewalls. ¿Le atrae más decodificar paquetes para interpretar lo que está pasando en el cable? ¿Mejor obsesionarse por encriptar todo lo que se escribe? ¿Prefiere implementar tecnologías o administrarlas? ¿Le gustaría ser el que define y establece las políticas de seguridad?

Csmo se puede ver hay una amplia variedad de carreras dentro de la seguridad.

Para que le sea más fácil elegir su área, considere presenciar una conferencia sobre seguridad. Va a conocer gente que ya está trabajando en el tema, obtendrá conocimiento, y puede llegar a establecer algunos contactos útiles.

Paso dos: Conocerse

En segunda instancia, psngase frente al espejo. Analice su formacisn, e periencia, aciertos y errores, sueños y realidades. Una clara interpretacisn de sus habilidades, aptitudes y e periencia es un buen punto de partida. Si establece un objetivo claro, podrá trazar el camino a seguir.

E periencia en administracisn de sistemas, networking o conocimientos sslidos de técnicas de programacisn son una buena base. Aunque muchos trabajos de seguridad no requieren configuracisn de sistemas o escritura de csdigo, si necesitan que usted entienda esas áreas. Es decir, la seguridad no puede ser el punto de partida para alguien que comienza a trabajar en IT.

Ahora las buenas noticias, una gran parte del trabajo en IT está relacionado con la seguridad. Los administradores de sistemas pasan una importante cantidad de tiempo concediendo y denegando accesos. La seguridad es en gran medida, ejercer control para prevenir el acceso a recursos.

Si en realidad a usted no le gusta pasar mucho tiempo tratando de que un sistema complejo quede afinado, o no le importa que su csdigo tenga buena performance, o directamente no le interesa el csdigo para nada, posiblemente, la seguridad no sea una buena eleccisn para usted.

Si, por el contrario, le parece que siempre hay alguien mirando sobre su hombro; si asume múltiples personalidades cuando está en línea; se suscribe a todos los newsletters de seguridad (y además los lee y sigue sus consejos), entonces probablemente está listo para tomar el camino de la seguridad.

Paso tres: Capacitarse

Aprender, certificarse, y adquirir e periencia, son los pasos dentro de la capacitacisn, y los primeros dos están en sus manos. En EE.UU. e isten incluso universidades que son designadas Centros de e celencia en educacisn de proteccisn de la informacisn y ofrecen programas de master y posdoctorados, algunas son: -Carnegie Mellon University, www.heinz.cmu.edu/infosecurity.

-George Mason University, www.isse.gmu.edu/~csis/inde .html.

-North Carolina State University, http://ecommerce.ncsu.edu/infosec/courses.html.

En Argentina se puede asistir a un programa de estudio en un instituto, donde, al igual que en el caso de las conferencias, encontrará gente con e periencia que lo pondrá en contacto con la realidad del trabajo de todos los días en seguridad. Estos programas están basados en los requerimientos de e ámenes de certificacisn, algunos de los cuales son:

CISSP (Certified Information Systems Security Proffessional - Profesional de Seguridad de Sistemas de Informacisn Certificado), por muchos considerada la certificacisn de seguridad. Es otorgada por el International Information System Security Certification Consortium (isc2.org)

SSCP (Security Systems Certified Practitional - Practicante Certificado en Seguridad de Sistemas), otorgado por la misma organizacisn. Tiene una orientacisn mas técnica y bastante nuevo.

CISA (Certified Information Systems Audit - Auditor de Sistemas de Informacisn Certificado), otorgado por la Information Systems Audit and Control Association. Es una certificacisn para auditores de sistemas, pero no para alguien que quiera convertirse en uno.

También e isten certificaciones específicas de algunos proveedores de soluciones informáticas (Recuadro).

Paso cuatro: Marketing

Una vez que se completaron los tres pasos anteriores, el cuarto deja de ser una tarea específica de la seguridad de sistemas, ahora tiene que salir a vender sus servicios, solo que ahora tendrá mas servicios para ofrecer. Destaque sus conocimientos y calificaciones en Seguridad y tendrá un importante valor agregado en su curriculum.

Como se ve, no es soplar y hacer botella , pero si está dispuesto a hacer el esfuerzo y, sobre todo, si decidis que se sentirá a gusto realizando tareas de seguridad informática, decídase, pronto habrá empresas que se den cuenta de que lo necesitan.

Proveedor	Site Web	Certificaciones
RSA Security	www.security.com/ training/certification	Certified Administrator Certified Engineer Instructor
Sniffer Technologies	www.sniffer.com/ education/scpp.asp	Certified E pert Certified Professional Certified Master
Symantec	www.symantec.com/ education/certification	Certified Security Engineer Certified Security Practitioner
Check Point	www.checkpoint.com/ services/education/ certification/inde .html	Certified Addressing E pert Certified Security Engineer Certified Security Administrator Certified Quality of Service E pert

Hacker, Cracker, Attacker, lammer, Kidie o simplemente perdido

Para no recibir críticas con referencia a la categoría de los intrusos, desde éste primer número vamos a dejar en claro que la perspectiva usada en las notas es la del administrador de sistemas y/o redes, por lo tanto en aquellas que traten temas de seguridad, por lo general se usarán los términos hacker , intruso , atacante , etc. como sinsnimos. ¿Porqué? Porque a un sysadmin no le importa si el intruso llegs para satisfacer su curiosidad sin límites, para mostrarse a él mismo o a sus amigos que podía hacerlo, para robar info., para destruir todo el sistema o para pedir trabajo en el área de seguridad de la empresa. Lo que al administrador le debe interesar es que **no e istan** accesos no autorizados al sistema, no importa si el que lo intenta es el mas 31337 de todos los hackers o un chico de 12 años que leys una nota en una e-zine y está probando, o si es alguien que quiso usar legalmente un servicio al que tiene acceso en un server cuyo IP es parecido al que posee el administrador de nuestro ejemplo, y se equivocs al tipearlo. Lo que interesa es que queden afuera los e traños.

Por supuesto que sabemos que el peligro varía de acuerdo al tipo de intruso que gane acceso no autorizado a un sistema, pero para eso, primero tiene que ingresar, y la intencisn del sysadmin es evitar que lo consiga para no tener que preocuparse por cuál es la filosofía del atacante.

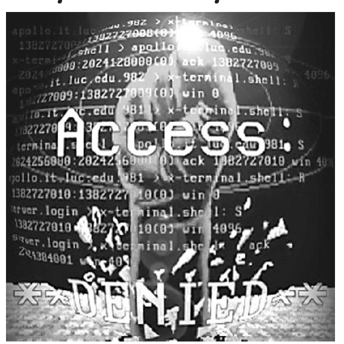
El punto de vista del intruso, sslo lo conoce él y puede variar durante la intrusisn, por ejemplo alguien que entra en un sistema solo por diversisn, podría verse tentado de sustraer informacisn si descubre que es interesante o valiosa.

a)Pequeño glosario

-Hacker: Alguien con verdaderos conocimientos de computacisn, ganados con la e perimentacisn, su intencisn no es hacer daño en los sistemas que intrusa, pero considera que la informacisn es de todos, de ésta forma, si algo le interesa lo toma. Muchas veces avisa al sysadmin del sistema hacheado para que éste corrija sus errores.

-Cracker: lleva un paso mas allá la idea de la propiedad de la informacisn, para el la informacisn no debe ser de nadie. Está mas cercano a la anarquía. Otro tipo de cracker es el que hace daño en los sistemas para demostrar poder.

-Lammer: Aprendiz de hacker. Le faltan conocimientos para acceder por las suyas



a sistemas ajenos, sslo usa herramientas, csdigos, bugs y backdoors descubiertos por otros. Por lo general no tiene mucho é ito y deja huellas de lo que estuvo haciendo.

-Kidie: lammer de corta edad.

-31337: élite, así se definen a si mismos los que se consideran los mejores hackers.

-e-zine: revista electrsnica publicada en Internet o BBS.

Diseño Web Pop Up

Una *popup window (ventana popup)* es una ventana del web-brouser que es más pequeña que las ventanas standards y sin algunos de los atributos standards tales como barras de herramientas o barras de status.

Popups son uno de los desarrollos mas complicados en desarrollo web. Mas de un desarrollador ha encontrado dificultades en su implementacisn. Aun mas, el uso irresponsable de técnicas de popup han dañado algunas paginas web e inaccesibles a los search engines .

Este tutorial nos guiará paso a paso en la creacisn de ventanas popup, incluyendo un juego completo de codigo JavaScript. Comenzamos con un ejemplo básico donde se muestran los elementos fundamentales de los popups. Luego mostraremos como establecer un link dentro del popup que nos lleve a la pagina principal. Luego recorreremos los muchos parámetros del comando open() que agrega muchas variaciones a sus popups.

Ventanas Popup: Lo Basico

Comenzaremos el tutorial creando una pagina popup básica. La técnica aquí descripta toca la mayoría de los temas en popups. El popup siempre viene al frente. Diferentes links pueden llevar a mismo popup. El csdigo es simple y fácil de modificar. Todo en este tutorial seran variaciones a lo descripto aquí. El csdigo en esta pagina crea un popup que se abre desde un link . Aquí mostramos el csdigo con la mínima descripcisn para ya funcione.

Primero copie este script en la <HEAD> section (seccion <HEAD>) de su pagina web:

```
<SCRIPT TYPE="te t/javascript">
<!--
function popup(mylink, windowname)
{
if (! window.focus)return true;
var href;
if (typeof(mylink) == 'string')
   href=mylink;
else
   href=mylink.href;
window.open(href, windowname,
'width=400,height=200,scrollbars=yes');
return false;
}
//-->
</SCRIPT>
```

Por ahora saltearemos los detalles de como funciona el script y pasaremos al siguiente paso. El script mas arriba abre el popup pero algo debe correr el script. La situacisn mas comun es que se ejecute cuando uno clickea un link. Un link como el que sigue haria correr el script

```
<A
   HREF="popupbasic.html"
   onClick="return popup(this, 'notes')">my
popup</A>
```

La mayor parte del link es lo usual. El URL de la pagina que es linkeada es el atributo HREF. Hemos agregado un atributo adicional llamado onClick. Copie o tipee el csdigo tal cual en su link con una sola modificacisn. El segundo argumento de popup() -- 'notes' indica el nombre de la popup window. Asegúrese de poner el nombre en tre *single* quotes ('). Así si quiere nombrar al popup 'stevie' use el csdigo como el que sigue

```
<A HREF="popupbasic.html" onClick="return
popup(this, 'stevie')">my popup</A>
```

Read This Ne t Part Or You'll Go Insane Trying to Figure Out Why Your Popup Doesn't Work
Lea esta parte o se volvera loco tratando de entender porque el popup no funciona.

Un pequeño pero importante detalle es a veces olvidado. El comando en onClick debe comenzar con return o el script file no funcionará.

```
onClick="return popup(this, 'notes')"
```

Ya hemos creado y abierto el popup. Pero uno de los problemas con popups es que una vez abierto se pasan al background. La primera vez que el usuario clickea el link el popup popea al frente pero si el usuario vuelve a clickear la pagina principal

Para evitar éste problema tenemos otra porcisn de csdigo. Este csdigo no va incluido en la página principal. Poner el siguiente csdigo en la página propia del pop up. Así, por ejemplo, el link anterior abre la página popupbasic.html , entonces el siguiente csdigo está en popupbasic.html , no en la página que está leyendo ahora

```
<SCRIPT TYPE="te t/javascript">
<!--
window.focus();
//-->
</SCRIPT>
```

Cuando la página del popup se carga, la script le dice al navegador que coloque el foco en el popup. Esto significa que el popup va al frente cada vez que se abre.

Esto es todo lo que hay respecto a los popups. De aquí en adelante es todo variaciones sobre el mismo tema.

Ventanas popup: Abrir automáticamente

En los primeros dos ejemplos se abre el popup cuando el usuario clickea un objeto. En éste ejemplo el popup se abre automáticamente

```
We'll use the same script as in the first
e ample. Copy this script A in the <HEAD>
section of your page.
```

Esta vez, en lugar de correr la script desde un link, lo haremos desde el atributo onload del tag <BODY >.

```
<BODY
onLoad="popup('autopopup.html', 'ad')">
```

El comando en onload se ejecuta cuando se termina la carga del documento. Csmo en nuestro ejemplo previo usa popup(), pero ésta vez el primer argumento para popup() es un poco diferente. En el anterior ejemplo pusimos this (éste), haciendo referencia al mismo link, y la script toms la URL desde el link. En este caso no hay link, así que le pasamos la URL real que debe abrir

Ventanas Popup: apuntando al origen

Una vez que se ha creado una ventana popup, hacer un link desde el popup hacia la ventana principal (la ventana que abris el popup) es un poco más complicado que lo que se podría pensar. El problema es que la ventana principal no tiene un nombre de la manera que lo tiene el popup. Afortunadamente, Javascript provee una respuesta en la forma de opener. Para crear links en la ventana popup que referencien a la ventana principal, primero hay que poner este javascript en el <HEAD> de la página del popup

```
<SCRIPT TYPE="te t/javascript">
<!--
function targetopener(mylink, closeme,
closeonly)
{
if (! (window.focus && window.opener))return
true;
window.opener.focus();
if (!
closeonly)window.opener.location.href=mylin
k.href;
if (closeme)window.close();
return false;
}
//-->
</SCRIPT>
```

Un link que usa esta script luce así:

```
<A
   HREF="rbe .html"
   onClick="return
targetopener(this)">Back to my my
page</A>
```

Ventanas Popup: Cerrando el popup

Si sslo se desea cerrar el popup sin hacer nada más, se debe agregar otro trae. Todavía hay que linkear a una URL válida en caso de que el usuario haya encontrado la página sin abrirla como popup.

```
<A
   HREF="rbe .html"
   onClick="return
targetopener(this,true,true)">close</A>
```

Ventanas popup: width & height

Width y height son propiedades requeridas solo para ventanas popup.

```
window.open(href, windowname,
'width=400,height=200,scrollbars=yes');
```

Ventanas popup: left & top

Left y top setean la posicisn del popup dentro de la pantalla. Si no se utilizan, entonces el navegador pone al popup donde quiera.

```
window.open(href, windowname,
'width=250,height=150,left=50,top=100,scr
ollbars=yes');
```

Las siguientes son las barras que podemos elegir mostrar o no en los popups. Todas son variables que se pueden setear en yes o no dentro del comando open(). Por default las barras no aparecen en los popups.

Ventanas popup: toolbar (barra de herramientas

Toolbar




```
window.open(href, windowname,
'width=400,height=150,toolbar=yes,scrollb
```

Ventans Popup: location (barra de direcciones))

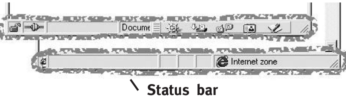


Location bar

```
window.open(href, windowname,
'width=400,height=150,location=yes,scroll
bars=yes');
```

Ventanas Popup: status (barra de estado)

La barra de estado muestra mensajes para el usuario. Por default los popups no tienen barra de estado.



Status bar
in MSIE and Nestcape

```
window.open(href, windowname,
'width=400,height=150,status=yes,scrollbar
s=yes');
```

Ventanas Popup: menubar (barra de menú)



menu bar

```
window.open(href, windowname,
'width=400,height=150,menubar=yes,scroll
bars=yes');
```


Ventanas Popup: scrollbars (barras de scroll)



Scroll bar

```
window.open(href, windowname,
'width=400,height=150,scrollbars=yes');
```

Ventanas Popup: resizable (cambiar tamaño)

```
window.open(href, windowname,
'width=400,height=150,resizable=yes,scroll
bars=yes');
```



Compartiendo con Samba

Samba es una herramienta que permite a los equipos UNIX LINUX interactuar con sistemas Windows. Lo que hace es permitir a aquellos sistemas compartir archivos utilizando el protocolo SMB (Session Message Block Bloque de Mensajes de Sesisn). Para un administrador esto significa que puede instalar un servidor UNIX sin tener que instalar NFS en todos los clientes Windows, porque estos van a utilizar su protocolo nativo SMB.

Samba es soportado por la mayoría de las variantes UNIX, por LINUX y por algunos sistemas no UNIX, es gratuito, está ampliamente documentado y por sus características facilita la administracisn de los servidores de archivos. Es todo eso lo que lo hace muy popular.

Aunque nacis como tal en 1995, su historia arranca realmente en 1992, cuando Andrew Tridgell se vio en la necesidad de acceder a archivos en una máquina Uni desde un PC. El cliente NFS (Network File System Sistema de Archivos de Red es el protocolo nativo de comparticisn de archivos Uni -Linu) que utilizaba trabajaba perfectamente, pero necesitaba también una aplicacisn que usaba la API de NetBIOS. Dada la problemática de usar protocolos múltiples bajo DOS, decidis adoptar un enfoque alternativo y utilizar la ingeniería inversa.

Mediante un *sniffer* monitores los paquetes transmitidos mediante SMB, desentrañs el protocolo y lo implements en su sistema Uni , capaz de manejar sin problemas varios protocolos de forma simultánea. Y eso fue el comienzo. Una vez depurado el csdigo, dado que el objetivo se había alcanzado, su desarrollo se detuvo. Este paréntesis durs hasta unos años después, cuando penss en conectar el PC con Windows de su esposa con su propia caja Linu . Dado que lo tenía a mano, probs su propio csdigo que, para su gran sorpresa, funcions perfectamente. Desde entonces, la esposa de Andrew se ha convertido en el primer test a que se someten las nuevas versiones de Samba, que es el nombre que se adopts para el paquete, buscando en un diccionario palabras con la combinacisn de letras smb.

Introduciéndonos

Samba es una emulacisn de NetBIOS, corriendo sobre Linu . Como tal, es un servicio que queda a la escucha sobre el puerto TCP/IP, 139.

Para realizar el camino inverso, es decir que Linu vea archivos compartidos por los servidores Windows, se utiliza la utilidad smbclient que forma parte del paquete Samba.

Para asegurarnos de que Samba esta instalado en nuestro sistema podemos usar el siguiente comando

[root@mail /root]# rpm -qa | grep Samba

Samba-2.0.6-20000313

Eso nos dice la versisn que está instalada

Si queremos saber que archivos pertenece a la instalacisn del paquete, podemos usar el comando

[root@mail /root]# rpm -qli Samba

Una e tensa lista nos dirá cuales son los archivos que pertenecen a Samba.

Configurando el servidor de Samba....

Aunque a partir de la versisn 2 del kernel de Linu se incorpors SWAT (Samba Web Administration Tool Herramienta de administracisn de Samba por Web) que consta de una interfase GUI (Graphic User Interface Interface Gráfica de Usuario) la configuracisn del servidor Samba la podemos hacer editando directamente el archivo /etc/smb.conf. Dependiendo de la distribucisn Linu que estemos usando, también puede encontrarse en /etc/Samba/smb.conf. Si tampoco se encuentra en ese lugar, lo podemos buscar con

[root@mail /root]# find / -name smb.conf



Configurando

El archivo de configuracisn fundamental de Samba, esta dividido en cuatro secciones Comenzaremos por la primera.

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this e  ample
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this e  ample we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.
#
# ================== Global Settings ==========================
[global]
# workgroup = NT-Domain-Name or Workgroup-Name
   workgroup = MYGROUP
```

Esto es fácil, debemos reemplazar MYGROUP por el nombre de workgroup o dominio que estemos utilizando.

```
# server string is the equivalent of the NT Description field
   server string = Samba Server
```

En éste lugar podemos poner lo que queramos, será el comentario de nuestro servidor.

La siguiente línea permite indicar el rango de direcciones IP de clientes autorizados a conectarse con el servidor

```
;   hosts allow = 192.168.1. 192.168.2. 127.
```

Pero como esta comentado, va a compartir toda la red.

```
# if you want to automatically load your printer list rather
# than setting them up individually then you'll need this
 printcap name = /etc/printcap
  load printers = yes
```

En esta seccisn, se nos permite indicarle a Samba que cargue las impresoras definidas en el archivo /etc/printcap (En ese archivo están definidas las impresoras y los msdulos)

```
 ;   printing = bsd
```

Linu usa el sistema de impresisn bsd, así que debemos descomentar ésta línea.

A continuacisn, seleccionaríamos si queremos utilizar una cuenta guest NO ES RECOMENDABLE

```
# Uncomment this if you want a guest account, you must add this to /etc/passwd
# otherwise the user "nobody" is used
;  guest account = pcguest
```

Con lo siguiente se configura Samba para generar un archivo de log (registro de actividades) distinto por cada máquina que se conecte

```
# this tells Samba to use a separate log file for each machine
# that connects
 log file = /var/log/Samba/log.%m
```

Y se le puede especificar el tamaño má imo de cada uno de esos archivos (es recomendable dejarlo como está)

```
 # Put a capping on the size of the log files (in Kb).
  ma   log size = 50
```

A continuacisn algo muy importante!

Samba permite cuatro tipos de seguridad.

share= comparacisn con cuenta guest

user = comparacisn a nivel grupo

server y domain, se utilizan a nivel dominio

Como utilizaremos la seguridad a nivel workgroup, sin cuenta guest, lo dejaremos así.

```
# Security mode. Most people will want user level security. See
# security_level.t  t for details.
   security = user
```

Si usáramos la seguridad del tipo server y domain, deberíamos poner aquí el nombre del Domain Controller (Controlador de Dominio) que queramos usar para realizar las autenticaciones

```
# Use password server option only with security = server
;   password server = <NT-Server-Name>
# Password Level allows matching of _n_ characters of the password for
# all combinations of upper and lower case.
;  password level = 8
;  username level = 8
```

Atencion aqui

Este es quizás el punto más importante de todo el archivo de configuracisn. A partir de Win95 OSR2, los passwords están encriptados. Anteriormente, esto no era así. Así que ahora, lo que debemos hacer es descomentar esto. Más informacisn la encontramos en la ayuda del paquete Samba.

```
# You may wish to use password encryption. Please read
# ENCRYPTION.t  t, Win95.t  t and WinNT.t  t in the Samba documentation.
# Do not enable this option unless you have read those documents
  encrypt passwords = yes
smb passwd file = /etc/smbpasswd
```

Pasemos a la siguiente seccisn.
#===================== Share Definitions ========================
[homes]
comment = Home Directories
browseable = no
writable = yes

Lo anterior define que cada usuario mantiene su profile en el home que indique su entrada en el archivo /etc/passwd.
NOTE: If you have a BSD-style print system there is no need to
specifically define each individual printer
[printers]
comment = All Printers
path = /var/spool/Samba
browseable = no
Set public = yes to allow user 'guest account' to print
guest ok = no
writable = no
printable = yes

Con esto le hemos dicho a Samba que queremos compartir las impresoras, pero que no le permita el acceso a las mismas al usuario *guest*.

Csmo siguiente paso vamos a definir un share (recurso compartido)
[Carpetageneral]
este será el nombre con el cual visualizaremos el recurso por NetBIOS
comment = Documentos comunes
#Ubicacisn física del directorio compartido
path = /usr/docs/
#Control de accesos al share
valid users = mbarrios, cpaina, fdomin

Con lo anterior compartimos el directorio local /usr/docs, con el nombre de recurso compartido Documentos comunes, al que tendrán acceso los usuarios mbarrios, cpaina y fdomin.
Si, quisiéramos permitir que el grupo Profesores acceda al share, lo haríamos de la siguiente manera.
valid users = @Profesores

Por ultimo, decimos que no sea un directorio público.
; public = no
después de guardar el archivo y salir del editor debemos ejecutar el comando *testparm*, para que haga una comprobacisn de que no hayamos ingresado cadenas que no sean reconocidas por Samba (por Ej.: suers en lugar de users)
[root@mail /etc]# testparm
Load smb config files from /etc/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Loaded services file OK.
Press enter to see a dump of your service definitions

Si e isten errores de sinta is nos lo irá diciendo.

Aun no tenemos corriendo Samba.

Para hacer funcionar el servicio debemos hacer es lo siguiente:
[root@mail /etc]# /etc/rc.d/init.d/smb start
Starting SMB services: smbd nmbd

Y ahí tendríamos corriendo Samba.

Para asegurarnos que el servicio está funcionando podemos ejecutar lo siguiente
(Recordar que Samba escucha en el puerto 139)
[root@mail /etc]# telnet localhost 139
Trying 127.0.0.1...
Connected to localhost.

Si la salida es esta, boila! , tenemos el servidor de Samba corriendo.

Últimos pasos:

Para validar los usuarios, Samba necesita además de que e istan como usuarios de sistema, generar los usuarios Samba. Esto se hace con el comando *smbpasswd*.
Si el usuario mbarrios no e iste en el sistema, lo podemos crear con
[root@mail /root]# useradd -m mbarrios

Luego, para crear la cuenta (usuario) mbarrios en Samba:
[root@mail /root]# smbpasswd -a mbarrios
New SMB password:
Retype new SMB password:
Added user mbarrios.
Password changed for user mbarrios

Con esto ya tenemos nuestro servidor Samba en funcionamiento.
Ultimo dato: la última versisn de Samba al momento de publicarse esto es la 2.2.4.

L I N K S
http://www.samba.org
http://www.insflug.org/COMOs/Samba-Como/Samba-Como-6.html
http://209.249.46.222/Linu /como-samba.php

¿Y para que necesito un Firewall?

Esta puede ser la pregunta de alguien que ha decidido dejar de pasar por alto la e istencia de ese algo que algunos mencionan: los Firewalls, y ahora se cuestiona si realmente quiere complicarse la vida estudiando, instalando y configurando uno de esos en su computadora o red.

Bueno, la verdad es que Internet es una gran maravilla, pero puede también ser un ambiente muy hostil. Afuera hay gente que puede estar interesada en la informacisn que usted tiene almacenada (personal, financiera, empresarial). Ahora bien, usted puede decir: -Me quedo tranquilo, nunca se me ocurriría tener informacisn comprometedora, ni números de tarjetas de crédito, ni mucho menos los secretos de mi é ito, guardados en una PC. No esté tan tranquilo, aún si no guarda nada en su computadora (cosa poco probable, para algo la tiene), todavía tiene algo interesante para los hackers: su computadora. En efecto, si el hacker quiere realizar ataques manteniendo oculta su propia identidad, puede poner las computadoras de otras personas a trabajar para el. Se puede dar el caso de que su PC este atacando el sitio Web de algún organismo sin que usted lo sepa. Se han dado casos de redes que estaban siendo utilizadas por e traños como depssitos de software ilegal, por supuesto que sin el consentimiento de los legítimos propietarios de la red.

Después de todo esto es posible que esté considerando que algún tipo de proteccisn de su perímetro puede ser necesario. Ahí es donde aparece el Firewall (pared de contencisn del fuego - cortafuegos).

Ahora bien, ¿Qué es en realidad? Una definicisn puede ser: Un Firewall es un sistema de seguridad que actúa como una frontera de proteccisn entre una red (o PC) y el mundo e terior .

Los Firewalls pueden ser piezas de software o hardware y son el equivalente a un guardia de seguridad, sslo que en este caso está apostado en la entrada/salida de su red. E isten cuatro tipos básicos de Firewalls, y estos son:

Packet filtering (Filtrado de paquetes)
Un Firewall de éste tipo acepta o deniega el paso del tráfico basado en los encabezados (headers) TCP/IP. Son los más baratos y también los que menos proteccisn brindan. Operan en la Networking layer (capa de red) del modelo OSI, no realizan chequeo del contenido de los paquetes y, como ventaja, casi no afectan la performance de la red.

Circuit-level gateway (gateway a nivel de circuito)
Estos Firewalls operan en la capa de sesisn (dos niveles más arriba que los Packet-filtering). En éste tipo, todas las cone iones (sesiones) son monitoreadas y solo a las que son consideradas válidas (por configuracisn) se les permite el paso. Esto generalmente quiere decir que un cliente detrás del Firewall podrá iniciar cualquier tipo de sesisn, pero los clientes e ternos no podrán conectarse a la máquina protegida.

Application-level Pro y (Pro y a nivel de aplicacisn)
Un Pro y es un representante, intermediario en la operacisn de comunicacisn. Estos Firewalls fuerzan a todas las aplicaciones de las estaciones de trabajo protegidas a que usen el Firewall como un Pro y. Para el cliente su servidor es el Pro y y el servidor ve al Pro y como su cliente. Entonces el Firewall puede autorizar cada paquete de cada protocolo en forma independiente. Sus desventajas son una perdida considerable en la performance de la red, y que aquellas aplicaciones que no puedan ser configuradas para utilizar un Pro y server, no funcionarán. La ventaja es el alto grado de seguridad que brinda.

Stateful Firewall (completo)
Estos Firewalls proveen un seguimiento y control del flujo de datos (entradas y salidas) de cada sesisn. La informacisn relativa a cada cone isn se almacena en memoria y, a medida que cada paquete llega al filtro, el Firewall toma la decisisn de pasarlo o bloquearlo usando la informacisn histsrica almacenada y una serie de reglas simples. El siguiente ejemplo del comando iptables causará que se bloquee el paso a cualquier paquete del protocolo icmp que sea recibido desde la interface loopback:
iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
(de iptables hablaremos en otra edicisn, por ahora solo va el ejemplo).

Un Firewall es un sistema de seguridad que actúa como una frontera de proteccisn entre una red (o PC) y el mundo e terior .



El ABC de Firewalls bajo Linu : uso de ipchains

Muy bien, si todavía sigue leyendo, parece que de verdad está interesado en el tema. Vamos entonces a analizar las opciones para configurar Linu Firewalls, corriendo Ipchains.
Ipchains es un Firewall de tipo Packet filtering.

Antes de empezar, los requisitos: ipchains funciona sslo con Kernels (núcleo del sistema) a partir de la versisn 2.2. . Si tiene un Kernel versisn 2.4 podrá correr en simultáneo ipchains e iptables.
Como ya dijimos, iptables es un Stateful Firewall, mientras que ipchains es un Packet Filtering Firewall. Si bien la semántica es parecida, internamente trabajan muy distinto e iptables es más poderoso. Aunque ipchains mantiene la ventaja de no afectar la performance de la red.

Cargar el Modulo de Ipchains

Si tiene un Kernel 2.2. , no necesita cargarlo. Si por el contrario, su kernel es versisn 2.4. , esto es lo que debe hacer:

#modprobe ipchains

Esto cargará el programa que nos permitirá editar las cadenas de filtrado.

Si deseamos conocer la versisn particular con la que estamos trabajando, lo podemos hacer con

#ipchains versisn

Puertos y servicios:

En el archivo /etc/services, encontraremos los puertos mas comunes que utiliza TCP

por ejemplo:

ftp-data	20
ftp	21
ssh	22
telnet	23
http	80
pop	110

Recomendacisn: Es bueno recorrer éste archivo para tener presente que puertos utilizan nuestro servicios.

Siguiendo con los controles, si al usar el comando

ping localhost

recibe la siguiente salida

Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TDV=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TDV=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TDV=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TDV=128

Su archivo /etc/hosts está bien configurado y la interface de loopback está respondiendo.

Establecer una nueva regla:

La versisn ipchains del comando iptable mencionado más arriba sería:

(notar que ipchains es case-sensitive (sensible a mayúsculas y minúsculas))

#ipchains A input p icmp s 0/0 d 127.0.0.1 j DENY

Si lo ejecuta (activa una regla en el Firewall), verá que los ping al localhost no serán respondidos.

¿Como se lee? (recordar que ejecutando *man ipchains* tenemos acceso a las páginas del manual de ipchains)

A = agrega una nueva regla en el firewall. En el caso del ejemplo, como se le agrega input , ésta es una regla que filtrará paquetes entrantes. Se pueden utilizar los siguientes parámetros:

-A	(Add new Rule) Agregar nuevas reglas
-D	(Delete Rule) borrar reglas
-N	(New Rule) Reglas definidas por el usuario
-X	(Delete user Rule) Borra regla definida por el usuario
-L	(List Rules) Lista reglas
-P	(Policies) Setea Politicas
-F	(Flush) Borra todas las reglas

-p = indica el protocolo cuyos paquetes serán analizados por ésta regla. En el ejemplo el protocolo es icmp (Internet Control Messages Protocol).

-s = establece la direccisn de origen (source) de los paquetes a ser filtrados. 0/0 usado en el ejemplo indica TODAS las direcciones.

-d = establece el destino (destination) que debe indicar un paquete para ser analizado bajo esta regla. En nuestro ejemplo 127.0.0.1, que es la direccisn de la interface de loopback.

-j = establece la accisn a llevar a ejecutar sobre los paquetes que cumplan con la regla. DENY indica que el Firewall NO dejará pasar los paquetes que cumplan con los requisitos establecidos en la regla.

Concepto de masquerading (enmascaramiento) o NAT

El Firewall también puede enmascarar las direcciones IP de los clientes dentro de nuestra red, de esa manera todos los hosts de su red e hibirán una única direccisn publica, aunque dentro de la Intranet mantengan sus direcciones privadas, esto esconde su red, esto también se llama NAT (Network Address Translation Traduccisn de direcciones de red). El comando es

#ipchains A forward s 192.168.1.0/24 j MASQ

Esto indica que los paquetes provenientes del network 192.168.1.0 con subset mask (máscara de subred) 255.255.255.0 (obviamente dentro de su red por tratarse de direcciones privadas) serán enviados a Internet mostrando csmo direccisn de origen la direccisn del servidor que provee el acceso a la Web.

Cerrando servicios:

Si se quisiera cerrar el acceso a un servicio determinado, pero no a todo el protocolo, lo que se debe hacer es cerrar el acceso al PUERTO que ese servicio utiliza:

#ipchains A input p tcp s superhackers.com d 200.200.200.200 21 j DENY

Donde superhackers.com es el origen a bloquear, 200.200.200.200 es la direccisn del server a proteger y 21 es el puerto a controlar. 21 es el puerto por defecto de ftp, y así está indicado en nuestro ejemplo del archivo /etc/services. Lo que se conseguirá con éste comando, es evitar que desde la direccisn superhackers.com se obtenga acceso por ftp a 200.200.200.200.

También se puede cerrar un conjunto de puertos, determinando un rango en la regla. Así

#ipchains A input p tcp s superhackers.com d 200.200.200.200 21:80 j DENY

Establecería la regla para los puertos desde el 21 hasta el 80.

Consultando las reglas:

Para listar las reglas que tenemos aplicadas en nuestro Firewall, el comando es simple:

#ipchains L

El resultado de éste comando puede parecerse a esto

Chain input (policy ACCEPT):
Target   prot opt   source   destination ports
DENY   icmp ------   anywhere
localhost   any -> any
Chain forward (policy ACCEPT):
Target   prot opt   source   destination ports
MASQ   all   ------
192.168.1.0/24   anywhere   n/a
Chain output (policy ACCEPT):

Borrando reglas:

Una forma de borrar reglas es

#ipchains D input p icmp s 0/0 d 127.0.0.1 j DENY

Este comando (con el parámetro D) borraría la primer regla que establecis en este tutorial (aquella que denegaba la recepcisn de paquetes dirigidos a localhost), es decir que a partir de este momento, si hace ping localhost o ping 127.0.0.1, tendrá respuesta.

Estableciendo políticas:

Establecer las políticas del Firewall es indicar de qué modo se comportará por defecto frente a los diferentes tipos de tráfico. Por ejemplo:

#ipchains A input DENY

Le dirá al Firewall que deniegue TODO el tráfico entrante, menos lo e plícitamente establecido (por otras reglas).

Guardando informacisn de eventos:

Hacer que el Firewall guarde un Log (registro de eventos) de lo que está ocurriendo es útil para saber que están accediendo o tratando de acceder los usuarios. Puede ser que se descubra que un usuario que tiene algún acceso denegado está tratando de usarlo (siendo rechazado por el Firewall), o que hay recursos que están siendo accedidos y que se ha olvidado de proteger. Los logs serán almacenados en /var/log/messages.

La forma de iniciar el logueo podría ser:

#ipchains A input j DENY l
#ipchains A output j ACCEPT l
#ipchains A forward j DENY -l

Esto causará que desde éste momento se comiencen a loguear los paquetes recibidos que fueron bloqueados, los salientes que fueron autorizados y aquellos a los que se les negs el forward.

Guardando y recuperando las reglas:

Todo lo que se ha hecho fue trabajo en memoria, si se desea contar con las reglas en sucesivos logins, se deben guardar las reglas en un file y esto se logra con

#ipchains-save > /sbin/firewall

Lo cual guardará la configuracisn del Firewall en el archivo /sbin/firewall

La forma de recuperar ésta configuracisn es

#ipchains-restore < /sbin/firewall

Ahora, basta de ejemplos sueltos, a continuacisn se muestra un Firewall sencillo implementado en un script usando ipchains:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
MAXI="192.168.0.201"
IPCHAINS="/sbin/ipchains"
$IPCHAINS -F input
$IPCHAINS -F output
$IPCHAINS -F forward
```



```
$IPCHAINS -A output -p tcp -d 0/0 www -t 0  01 0  10
$IPCHAINS -A output -p tcp -d 0/0 telnet -t 0  01
0  10
$IPCHAINS -A output -p tcp -d 0/0 ftp -t 0  01 0  10
$IPCHAINS -A output -p tcp -d 0/0 ftp-data -t 0  01
0  08

$IPCHAINS -A input -p tcp -s 0/0 -d 0/0 1023:65535 -j
ACCEPT
$IPCHAINS -A input -p udp -s 0/0 -d 0/0 1023:65535 -
j ACCEPT
$IPCHAINS -A input -p tcp -s $MAXI -d 0/0 20 -j
ACCEPT
$IPCHAINS -A input -p tcp -s 192.168.0.231 -d 0/0 20
-j ACCEPT
$IPCHAINS -A input -p tcp -s $MAXI -d 0/0 21 -j
ACCEPT
$IPCHAINS -A input -p tcp -s 192.168.0.231 -d 0/0 21
-j ACCEPT
$IPCHAINS -A input -p tcp -s $MAXI -d 0/0 23 -j
ACCEPT
$IPCHAINS -A input -p tcp -s $MAXI -d 0/0 25 -j
ACCEPT

#Reglas Icmp

$IPCHAINS -A output -i eth0 -p icmp -s 0/0 -d 0/0 -j
ACCEPT
$IPCHAINS -A output -i eth0 -p icmp -s 0/0 -d 0/0 -j
ACCEPT
$IPCHAINS -A input -i eth0 -p icmp -s 0/0 -d 0/0 -j
ACCEPT
$IPCHAINS -A input -i eth0 -p icmp -s 0/0 -d 0/0 -j
ACCEPT

$IPCHAINS -A input -j DENY
$IPCHAINS -A output -j ACCEPT
$IPCHAINS -A forward -j DENY
```

Como verán aquí, es mas sencillo utilizar variables, por si nos cambia una IP, no debería afectar a todo el firewall.

Esperamos haberle facilitado un encuentro amigable con los conceptos de Firewall. La presentacisn de la herramienta ipchains nos sirvis para demostrar que la seguridad de una red no tiene por que ser costosa, aunque si puede haber grandes pérdidas cuando no se aplica. Si le interesa ver una descripcisn mas detallada de los comandos ipchains y un ejemplo de la configuracisn paso a paso de un Firewall en una red, por favor visite www.ne .com.ar (OnLineDoc 0000 000).

L I N K S

http://www.netfilter.org/ipchains/spanish/HOWTO.html#toc7

Pregunta de Linu + / LPI

¿Cuál de los siguientes commandos, protégé el archivo calculos , para evitar que sea borrado incluso por root?

a) **chattr** +c **calculos**
b) **chattr** +i **calculos**
c) **chmod** 000 **calculos**
d) **chmod** a-rw **calculos**

Respuesta

La respuesta correcta es la b. Cuando se usa el comando chattr +i calculos, dicho archivo queda protegido de ser borrado. Este comando setea el atributo "inmutable" para el archivo "calculos". Ni los usuarios regulares ni root pueden borrar, modificar o renombrar un archivo con el atributo "inmutable" seteado. Tampoco se pueden crear links a un archivo con dicho atributo seteado. Sslo root puede establecer y quitar éste atributo. Para quitar el atributo "inmutable" se debe usar el comendo chattr -i calculos. Después de haber hecho eso, el archivo se podrá borrar.

el comando chattr +c comprime el archivo. Los comandos chmod 000 calculos y chmod a-rw calculos quitan los atributos read, write y e ecute del archivo calculos, pero todavía el dueño del archivo y root

eventos

Agosto de de 1991

"Hello everybody out there using Mini estoy desarrollando un sistema operativo (gratis), (sslo es un hobby, no va a ser grande y profesional como GNU) para clones AT 386(486). Se ha estado cocinando desde abril, y está empezando a quedar terminado. Me gustaría recibir algún feedback sobre cosas que a la gente le gusta o disgusta de Mini , como mi SO se le parece un poco (la misma disposicisn física del sistema de archivos (por razones prácticas) entre otras cosas).

Actualmente, he migrado bash (1.08) y gcc (1.40), y las cosas parecen funcionar. Esto implica que voy a obtener algo práctico dentro de pocos meses, y me gustaría saber que características desea la mayoría de la gente. Todas las sugerencias son bienvenidas, pero no prometo que las vaya a implementar :-)

Linus (torvalds@kruuna.helsinki.fi)

P.D.: Sí - está libre de todo csdigo Mini , y tiene un sistema de archivos Multi-threaded. No es portable (usa el cambio de tareas del 386 etc.), y probablemente nunca de soporte a nada más que a los discos rígidos para AT, porque eso es todo lo que tengo :-(."

-Lo anterior es la primera mencisn de LINUX en la red, es el mensaje que Linus Torvalds aviss que estaba desarrollando el SO mas revolucionario, evidentemente, sin saber que su SO de hobby iba a hacer tanto ruido y crecería de la forma que lo ha hecho.

LAS 10 CERTIFICACIONES MAS BUSCADAS DEL MERCADO

**En un articulo de certcities.com se discutis cuales serán las certificacisnes de más interés durante el 2002. (10 hottest certifications)
http://certcities.com/editorial/features/story.asp?EditorialsID=37
Lo interesante del artículo es que se baso en crecimiento, reputacisn, y aceptacisn de la industria. Esto agregado a otros factores: utilidad, ¿puede hacer una diferencia en la carrera?, cual brillará más. En particular nos referiremos a aquellas que creemos podrán impactar el mercado Argentino, aunque conocer el impacto afuera también puede ser de mucho interés.**

10
Certified Information Systems Security Professional (CISSP)
Vendor: **ISC2**
Category: **Security**
Reader Interest Score (out of 20): **7**
Buzz Score (out of 10): **9**
Total: **16**

9
Sun Certified Java Programmer (SCJP)
Vendor: **Sun Microsystems**
Category: **Programming**
Reader Interest Score (out of 20): **12**
Buzz Score (out of 10): **5**
Total: **17**

8
Citri Certified Administrator (CCA)
Vendor: **Citri**
Category: **Networking**
Reader Interest Score (out of 20): **11**
Buzz Score (out of 10): **7**
Total: **18**

7
Network+
Vendor: **Computer Technology Industry Association (CompTIA)**
Category: **Networking**
Reader Interest Score (out of 20): **16**
Buzz Score (out of 10): **4**
Total (out of 30): **20**

6
Red Hat Certified Engineer (RHCE)
Vendor: **Red Hat**
Category: **Linu**
Reader Interest Score (out of 20): **14**
Buzz Score (out of 10): **7**
Total: **21**

5
Microsoft Certified Database Administrator (MCDBA)
Vendor: **Microsoft**
Category: **Database**
Reader Interest Score (out of 20): **20**
Buzz Score (out of 10): **2**
Total: **22**

4
Cisco Certified Network Professional (CCNP)
Vendor: **Cisco**
Category: **Networking**
Reader Interest Score (out of 20): **16**
Buzz Score (out of 10): **7**
Total (out of 30): **23**

3
Cisco Certified Network Associate(CCNA)
Vendor: **Cisco**
Category: **Networking**
Reader Interest Score (out of 20): **18**
Buzz Score (out of 10): **6**
Total: **24**

2
Oracle Certified Professional Database Administrator (OCP DBA)
Vendor: **Oracle**
Category: **Database**
Reader Interest Score (out of 20): **18**
Buzz Score (out of 10): **7**
Total: **25**

1
Microsoft Certified Systems Administrator (MCSA)
Vendor: **Microsoft**
Category: **Networking**
Reader Interest Score (out of 20): **18**
Buzz Score (out of 10): **8**
Total (out of 30): **26**

Certificaciones MCP

MCP	813.533
MCSE	478.983
MCSD	35.897
MCT	13.336
MCDBA	69.426
MCSA	22.329
MCP+Internet	229.160
MCP+Suite Building	2.017
MCSE+Inetnet	12.388
Nº de Certificaciones	1.677.089

El Crucero de la Certificación

¿Como preferiría obtener su MCP: leyendo libros y manoseando una red casera en su sstano sin ventanas o en un crucero equipado alrededor de Jamaica y las Islas Caimán?

Esta es la pregunta que Neil Bauman espera que se haga, y es por eso que agrego certificaciones Microsoft a sus otros ofrecimientos en Geek Cruises.

Geek Cruises comenzs hace dos años, con un viaje para programadores Perl. Fue tan e itoso que Bauman adiciono otras especialidades informáticas, incluyendo programacisn en Java y Linu . Certification Sail , como llama él al crucero MPC, es su más reciente oferta. Es una e cursisn de siete días, empezando en Tampa, Florida y serpenteando hacia Cozumel, Mé ico.

En los viejos días, una vez que pasabas la prueba MCP, podías esperar obtener un aumento de sueldo del 10 por ciento , dice Bauman. Y tenías que pagártelo vos mismo. ¿Si tiene qué pagárselo usted mismo, preferiría pasar 40 horas en Idaho o en el Caribe?, es lo que Barman pregunta

El crucero tiene tres días completos en alta mar, y es ahí cuando la mayor parte del entrenamiento es hecho. Se pasa cada uno de esos días entrenando desde las 8 de la mañana hasta las 8 de la noche. El programa tiene como objetivo ayudar a pasar dos pruebas MCE: 70-210, Windows 2000 Profesional , y 70-215, Windows 2000 server . Los vamos a presionar duro les dice Bauman a los estudiantes.

Sin embargo, ¿qué tan duro? ¿No sería fácil distraerse en un crucero? No para la audiencia a la que apunta, según Bauman. En el barco hay cuartos que no tienen ventanas, y es donde probablemente hagamos esto. Cuando está en alta mar, tiende a ser aburrido. [Ellos] encontrarán que esto es lo ideal para pasar el tiempo en alta mar. En Alaska, el tiempo en el mar es hermoso. En el Caribe, todos lo que ves es agua. Y luego de verlo por un rato no necesita seguir viéndolo.

Los cruceros tienen otra cosa que contribuye al aprendizaje, Bauman señala: Están fuera del mundo. Beepers y teléfonos celulares no funcionan en alta mar.

Aunque la certificacisn Microsoft empieza despacio, ofreciendo solo dos e ámenes, Bauman dice: Hay una oportunidad del 100 por ciento de que ofrezcamos más certificaciones. Actualmente está estudiando certificaciones .NET, que probablemente lanzará a fines de este año o principios del prs imo.

Entonces, ¿qué puede ser mejor que obtener la certificacisn en el Caribe?

Consiguiendo que el jefe pague por él. Bauman incluso tiene sugerencias de como abordar a su jefe. Está propagándose la palabra de que éstos son cruceros prestigiosos. El crucero en si no es caro, comúnmente $ 1000, incluyendo comida y alojamiento por siete noches

Se puede encontrar más sobre Geek Cruise en www.geekcruises.com



Artículo publicado en la revista MCP Magazine de Agosto de 2002.-

Si bien lo que en el artículo se considera barato (u$s 1.000), desde la devaluacisn para nosotros es más que oneroso, y tampoco contamos (por ahora) con cruceros de la certificacisn , en nuestro país tenemos la ventaja de que los costos de los cursos son innegablemente mucho mas baratos que los que se pagan en el gran país del norte. Y es que en Argentina, se puede llegar a realizar la carrera MCSA por alrededor de u$s 400.- más los 4 e ámenes (u$s 360) y éstas certificaciones tienen la misma validez que las obtenidas en Idazo, Florida o donde sea. No nos podemos comparar con ellos, pero eso, para los que saben buscar, es una gran fuente de oportunidades.

Publicidad
COLOR

Publicidad
COLOR

Publicidad
Color